

思科系统公司子公司



2.4GHz Wireless-G

VPN 宽带路由器 WRV54G-CN

用户手册

版权和商标

如何使用本手册？

本手册中所涉及的“Wireless-G VPN 宽带路由器”是根据网络设计的，它的使用方法比路由器更为便捷和高效。在阅读本手册时，敬请注意下列事项：



这个确认符号是一种友情提示符号，意思是当你在使用路由器时要特别注意的一些事项。



这个三角感叹符号意思是警告你某些硬件会遭损坏或路由器会遭损坏。



问号是向你提供一些路由器使用过程中必要的解释信息。

除了这些符号之外，还有一些技术术语按照以下格式显示：

术语：定义

除了上述内容之外，还会有一些图示（树状图，点击图，或其他图片），上面会附有图片编号和说明，具体格式如下：

图 0-1：样品图示说明

在目录中的图片一览表里，您还能浏览图片编号说明。

目录

第 1 章：简介 1
  欢迎 1
  本手册是什么？ 2
第 2 章：布局规划的无线网络 4
  路由器的功能 4
  IP 地址 4
  需要 VPN 网络的原因？ 5
  VPN 的定义？ 6
第 3 章：了解 Wireless-G 宽带路由器的基本构造 9
  背板 9
  前面板 10
第 4 章：Wireless-G 宽带网络路由器？ 11
  综述 11
  有线连接到一台计算机 12
  无线连接到一台计算机 12
第 5 章：计算机的系统配置 14
  综述 14
  对 Windows 98 进行参数设置 14
  对 Windows 2000 操作系统的计算机进行网络设置 15
  对 Windows XP 操作系统计算机进行参数设置 16
第 6 章：配置路由器 18
  综述 18
  如何访问网络为基础的实用程序 20
  安装标签 20
  无线标签 27
  安全标签 31
  访问限制标签 36

应用程序及对策标签 38
管辖标签 42
状态 46
附录 A：疑难问题解答 49
一般问题的解决 49
常见的问题解答 57
附录 B：无线安全 64
概述 64
危险是什么？ 64
附录 C：配置 Windows 2000 计算机和路由器之间的互联网协议安全 71
引言 71
环境 71
如何确立一个安全的互联网协议安全隧道 72
附录 D：找出以太网适配器的 MAC 地址和 IP 地址 82
Windows 98 或 Me 指令 82
Windows 2000 或 XP 指令 83
附录 E：SNMP 功能 84
附录 F：升级固件 85
附录 G：Windows 帮助 86
附录 H：词汇表 87
附录 I：技术说明 93
附录 J：保修信息 95
附录 K：规章信息 96
附录 L：联系信息 97

第一章：简介

欢迎

无线 G 是 54Mbps 无线网络标准的升级，它比广泛运用于家庭，企业和公共场合的无线 B 标准产品网速快将近 5 倍，但另一方面，由于它同样运用 2.4GHz 的无线波段，所以无线 G 设备可以兼容 11Mbps 网速的无线 B 设备。

基于两种网络标准的兼容性，您不必重复投资，可以将原先的无线 B 标准的设备用在无线 G 网络上，这样可以大大提高您的网速而不必投资很多。

Linksys 公司的无线 G 宽带路由器是一个带有三个设备的机盒。首先，有一个无线接入器，它的功能是把无线 G 或无线 B 的设备与网络相连。盒子内还有一个内置的四端口双向 10/100 的交换器，它是用来连接有线的以太网设备，进一步说就是把四台计算机直接或间接的与更多的 HUB（集线器）和交换器相连，从而形成一个你所需要的大型网络。最后，还有一个路由器功能，它与所有设备相连，它的功能是让整个网络共享高速的光缆传输或 DSL 互联网传输连接。

为了保护您的数据安全和隐私，无线 G 宽带路由器向您提供了各种无线传输方式的加密功能。这种宽带路由器具有 DHCP 服务器的功能，运用了 NAT 技术来保护您的数据，防止那些黑客的侵入，同时保持信道的畅通，它也可以与过滤器相连，使内部用户轻松的接入互联网。这一功能可以通过基于网络浏览器配置的编程来完成。

随着 LINKSYS 无线 G 宽带 VPN 路由器在家庭和办公中心网络的使用，你能享受到高速的网上冲浪，快速的打开共享文件，使用打印机，还有灵活快速玩多人电脑游戏，同时又可以保障网络安全。

本手册是什么？

用户手册包含了安装，设置和使用无线 G VPN 宽带路由器的步骤。

第一章 简介
这一章讲述了无线 G VPN 宽带路由器应用程序和用户手册。

第二章 无线网络的基本布局和规划
这一章讲述了无线网络工作的基本原理和流程。

第三章 无线 G VPN 宽带路由器的物理构造
该章介绍了此种路由器的一些物理功能。

第四章 无线 G 宽带路由器的连接
指导你如何正确把路由器与你的网络相连。

第五章 计算机所需的系统配置
这一章讲述了使用宽带路由器时，计算机方面所要的系统配置。

第六章 路由器本身的参数设定
本章解释了如何根据网络对路由器进行功能参数设定。

附录 A: 常见问题解决
该附录给出了一些安装调试使用过程中常见问题及解决方法。

附录 B: 无线网络安全
该附录阐明了无线网络运行的危险性和减少危险的一些具体措施。

附录 C: 在 WINDOWS 2000 计算机端与路由器配置 IP 地址连接中的安全措施
该附录指导你如何运用 IP 地址安全策略，利用设定键，把 VPN 路由器虚拟个体网络与 WINDOWS 2000 或 XP 操作系统下的计算机终端相连接。

附录 D：SNMP 功能
解释了什么是 SNMP

附录 E：路由器功能升级
指导你如何对路由器进行功能升级。

附录 F：WINDOWS 帮助
指导你如何利用 WINDOWS 系统中帮助部分的网络部分，例如安装 TCP/IP 协议。

附录 G：为你的以太网适配器找到 MAC 地址和 IP 地址
该附录讲述了如何为你的计算机上的以太网适配器找到 MAC 地址，也就是说运用 MAC 过滤功能和路由器地址定位功能去寻找 MAC 地址。

附录 H：术语表
给出了网络中常用的专业术语

附录 I：技术规格书
该附录给出了该路由器的技术规格参数

附录 J：品保书
提供了该路由器品保信息。

附录 K：常规信息
提供了路由器相关的常规信息

附录 L：连接方式
该附录提供了 LINKSYS 集团各部门的联络方式包括技术支持部门的联络信息。

第二章：布局规划你的无线网络

路由器的功能：

简而言之，路由器就是把两个网络连接在一起的设备。

也就是说，路由器就是把你的局域网或家里或办公室一群计算机与国际互联网相连。路由器处理和规范两边网络的数据。

路由器的 NAT 功能保护你的计算机网络，所以当用户在公共场合，互联网那一端看不见你的计算机。这几使你的网络保持私属性。你的路由器会在数据传输到正确的计算机端时，检查每一个通过互联网端口的数据包，以确保你的网络安全。路由器也检查互联网端口服务，例如 WEB 服务器，FTP 传输协议服务器，或其他互联网应用程序，如果允许通过，那么数据包会准确到达局域网的计算机端。

记住了路由器端口连接的是两边。局域网端口连接局域网这一端，互联网端口连接的是互联网这一端。局域网和互联网端口是以 10/100Mbps 的速度来传输数据的。

IP 地址

IP 地址定义?

IP 是互联网 PROTOCOL 的缩写。每一个设备都是基于 IP 协议网络的，包括计算机，打印服务器，路由器，他们都需要 IP 地址以确认他们在网络上的位置或地址。这运用到局域网和互联网的连接上。获得 IP 地址的方式有两种：固定 IP 地址和运用路由器获得动态 IP 地址。

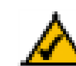
固定 IP 地址：

一个固定 IP 地址是一个固定的 IP 地址，通过手动赋予计算机或其他网络上的设备。一个固定 IP 地址会一直有效除非你停止使用此地址，也就是说固定地址获得以后，网络一直会使用同一固定地址去识别该设备，除非你去认为改变它。固定 IP 地址必须具有唯一性，一般运用与网络设备例如计算机服务器和网络打印服务器。



图 2-1：网络

局域网（LAN)：由众多计算机和网络设备组成的局域网络。



注释：由于路由器是连接两个网络的设备，所以它需要两个 IP 地址----一个为局域网，一个给互联网。在这个用户手册里，你将看到“互联网 IP 地址”和“局域网 IP 地址”方面的指导。

由于此种路由器用的是 NAT 技术，互联网上仅能看到路由器的互联网 IP 地址。但是，即使这个互联网 IP 地址能被阻挡，以便互联网上看不到路由器和网络---可以查阅第七章：“路由器基于网络的御用”中“运用过滤器阻碍 WAN 请求”。

如果你想用路由器共享你的光缆和 DSL 互联网连接，你可以查你的 ISP 确定你是否赋予你的帐户一个固定 IP 地址。如果有，当你设置路由器的时候，你将需要固定 IP 地址。你可以从 ISP 上得到这方面的信息。

动态 IP 地址:

一个动态 IP 地址是设备在网络上自动获取的，例如计算机和打印服务器。这些 IP 地址被称作动态是因为他们都是暂时赋予计算机或其他设备的 IP 地址。一段时间后，这些动态 IP 地址会过期失效或改变，DHCP 服务器将会给它一个新的动态 IP 地址。

DHCP（动态主机配置协议）服务器

DHCP 服务器赋予了计算机和其他网络设备动态 IP 地址。获得 DHCP 服务器提供的动态 IP 地址的计算机或网络设备我们把他们称作 DHCP 的客户端。当有新用户加入，DHCP 服务器免去您手动给予 IP 地址的麻烦。

DHCP 服务器即可以是网络上指定的计算机或是其他的网络设备，例如路由器。通过默认设置，路由器的 DHCP 服务器功能可以被激活。

如果你的网络上已经有了一个 DHCP 服务器，你必须关闭其中一个 DHCP 服务器。如果你在网络上运行不止一个 DHCP 服务器，你将会遇到网络错误，例如 IP 地址冲突。如何关闭路由器上的 DHCP 功能，见“第六章: 路由器网络运用”中 DHCP 功能部分。

需要 VPN 网络的原因？

计算机网络提供了灵活的使用环境，这是古老的基于纸张的信息传输系统所不具备的。这种灵活性也带来了负面影响，危险性也增加了。这就是为什么要使用防火墙。防火墙用来保护网络内部的数据。但是如何保护发到外面的数据，当发 E-MAIL 到外部网络，或在公司外部与公司网络相连？你该如何保护你的数据？

VPN 由此应运而生，VPNS 是 VIRTUAL PRIVATE NETWORKS 的缩写，意思是虚拟隐私网络，他把传到网络外部的数据也虚拟看作依然在局域网络内。

当数据从你的计算机上被传到互联网上时，总是很容易受到攻击。你也许已经有了一个防护墙，但是它只能防止内部数据不被侵扰，或不让外部不良数据进来，但是一旦数据出了你的局域网，例如你把数据送到外部邮箱或和别人在互联网上聊天，这时防火墙不再保护你的那些数据。

从这一点意义上看，你的数据很容易受到黑客的攻击，他们可以偷走你传输的数据，还有你的登陆密码或安全数据。一些最常规的手段如下：

1） 盗用 MAC 地址
你局域网或互联网上传输的数据包都有一个数据包台头。这些台头包含了数据来源和目的地信息，为了使传输更高效。一个黑客可以用这个信息伪造一个 MAC 地址，来盗用该数据，也可以把该数据传到另外的用户上。

2） 吸入数据
数据吸入是黑客常用的方法，他们通过不安全的网络来获取信息例如互联网。有很多这样的网络工具，例如传输协议分析器，网络诊断工具，进入操作系统，可以清楚的浏览数据。

3） 网络攻击者
一旦黑客吸取了或盗用了足够的信息，他就能发动网络攻击。他可以改变数据传输的路径，可以截取数据，让数据到达不了收件人。

这里仅讲述了几种黑客攻击的方式，黑客也在不断发展他们攻击方式。没有 VPN 的安全措施，你的数据会在网上传输时随时受到攻击。数据在最终到达指定服务器是会通过很多不同的服务器。也就是说数据会相当容易受攻击，这就是 VPN 使用目的。

VPN 定义？

VPN 是 Virtual Private Network 的缩写，它连接了两个终端点---一个 VPN 路由器，举个例子---在不同的网络里允许个人的数据在共享或公用网络里传输，例如互联网。这就需要建立一种隐私网络，可以使数据在两个位置或网络间传输。

我们可以建立这样一种数据通道。一个 VPN 数据通道连接了两台计算机或两个网络，它允许数据通过互联网传输，就好象仍然在他们的网络内部。它不是我们书面上说的隧道，而是一种安全连接方式，给网络间传输的数据加密。

VPN 是一种使用个人网络，专用网络或租用网络时保护网络安全非常行之有效的方法。运用工业标准加密认证技术——IP 安全认证——VPN 创建

一个安全连接，实际上就好象你直接和你的局域网相连。VPN 被用来创立主次办公地点之间的网络连接，实现了远程办公，在路上也可以办公。（旅行者把计算机连到 VPN 路由器上，用支持 IP 安全策略的 VPN 客户端软件，就可以实现远程办公，例如 SSH 信号发射器。）

有两种基本的方式来创立 VPN 连接:

- VPN 路由器——VPN 路由器;
- 计算机（有 IP 安全策略支持的 VPN 客户端软件）——VPN 路由器

VPN 路由器在两个末接点创建了一个通道，以便两个网络之间的数据可以安全传输。一台带有 IP 安全策略支持 VPN 客户端软件的计算机也可以成为两个末端节点中的一端。任何带有 IP 安全管理器的计算机（WINDOWS 2000 和 XP）都允许 VPN 路由器运用 IP 安全策略创立一个 VPN 数据通道（见“附录 C：运用 IP 安全策略连接 WINDOWS 2000 或 XP 计算机与 VPN 路由器”）。其他版本的 MICROSOFT 操作系统需要额外的，第三方 VPN 客户端软件应用程序支持 IP 安全策略的安装。

VPN 路由器——VPN 路由器
下面以图解举例说明此种连接。（见图 2-2）在家里，一位远程办公人员用自己的 VPN 路由器总是与 INTERNENT 连接。他的路由器使用他办公室 VPN 设置。当他与办公室的路由器连接时，这两台路由器就创建了自己的数据通道，加密，解密他们的数据。当 VPNS 运用互联网时，距离不是关键因素。使用 VPN 连接，远程办公人员就可以随时安全与办公室的网络连接，好象有一种恰在其办公室的感觉。



图 2-2：



重要提示：你在数据通道的两端至少有一台 VPN 路由器。另一端，可以是 VPN 路由器或装有基于 IP 安全策略 VPN 客户端软件的计算机。

计算机（装有 IP 安全策略支持的 VPN 客户端软件）——VPN 路由器

以下我们用图解举例说明此种连接。（见图 2-3）在她的酒店客房里，一个商务旅行的女商人拨打了她的 ISP。她的笔记本电脑上装有 VPN 客户端软件，并且使用办公室的 VPN 设置。她打开了 IP 安全策略支持的 VPN 客户端软件，与中心办公室的 VPN 路由器连接。当 VPNS 使用互联网，距离不是问题。使用 VPN 连接，女商人现在有了与中心办公室网络的安全连接，就好象在办公室里一样。

要想了解更多如何建立你自己 VPN 信息指导，请访问 LINKSYS 的网站，www.linksys.com 或参阅“附录 C：配置 IP 安全策略连接 WINDOWS 2000 或 XP 系统的计算机与 VPN 路由器”。



图 2-3：

第三章：了解 Wireless-G VPN 宽带路由器的基本构造

背板:

路由器的端口，网络连线口位于背板上。

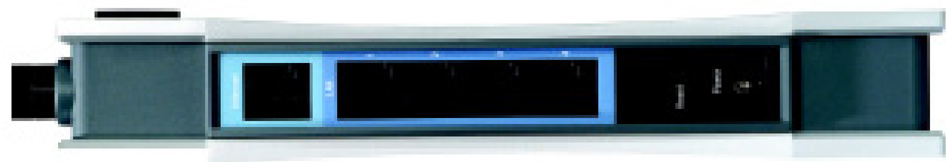


图 3-1：背板

互联网端口 互联网端口与你的调制解调器相连
局域网（1-4） 局域网端口，连接你的计算机和其他网络设备
电源 电源端口连电源适配器
复位键 有两种方式重设路由器的默认设置。一种是按 RESET 键，大约要 10 秒，还有一种是在路由器网络运用模块里恢复默认设置。

除此之外，还有其他的 LINKSYS 产品，可以无限扩冲您的网络功能，请访问 www.linksys.com 获得有关路由器产品的更多的产品信息。

重要提示：复位路由器将永久删除你的设置(WEP 加密设置，无线和局域网设置等等）并且用默认设置取代它。如果你想保留原由设置，不要使用复位键。

前面板

路由器的网络运行状态信息都显示在前面板上。

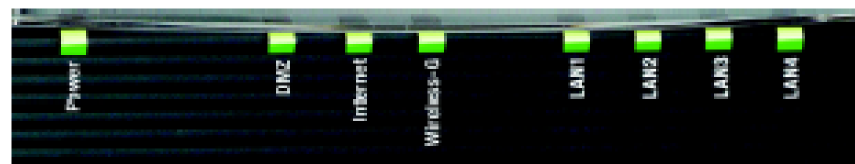


图 3-2：前面板

电源指示灯　　绿色。当电源打开，电源灯显示绿色。

DMZ　　红色。DMZ 提示灯接入点在引导程序启动时做自我诊断测试并重启。测试诊断完成后灯熄灭。如果该灯持续时间过长，请参阅附录 A：错误诊断

互联网指示灯　　绿色。无论何时无线连接成功，互联网提示灯都会亮启。如果指示灯闪烁，表明路由器正从网络设备或计算机上接受或发送数据。

无线 G 指示灯　　绿色。无线 G 提示灯在无线连接成功后亮启。

局域网指示灯（1-4）　　绿色。局域网指示灯有两个目的。如果指示灯一直亮着，表明路由器成功通过局域网端口与一台设备相连。如果指示灯闪动，表明有一些网络活动。

第四章：Wireless-G 宽带网络路由器

综述：

路由器的安装不但包含即插型硬件的安装，你不得不重新配置你的网络计算机，以便接收路由器赋予它的IP 地址（如果在用），并且你也要不得不用互联网服务供应商提供的数据对路由器重新配置。

网络服务供应商的安装技术人员应该会在装好宽带后，把调制解调器的设置安装信息给你，如果没有你可以打电话给网络供应商索要相关信息。

一旦你有了你需要网络类型的设置安装信息，你就可以开始安装设置路由器了。

如果你想用带有以太网适配器的计算机去配置路由器，继续用有线连接到计算机。
如果你想用带有无线适配器的计算机去配置路由器，继而用无线连接到一台计算机。

有线连接到一台计算机：

1 在开始连接之前，确认你的网络硬件设备处于断电状态，包括路由器，计算机，光缆或 DSL 调制解调器。

2 把以太网网络光缆的一个末端连到局域网一个端口上（标签 1-4），在路由器背板上（见图 4-1），另一端连到计算机上的以太网端口上。

3 重复这个步骤，连接更多的计算机，一个交换器，其他的网络设备到路由器上。

4 从你的光缆或 DSL 调制解调器上拉一个不同的以太网网络光缆线到路由器面板上的互联网端口上。这是连接你的调制解调器唯一有效端口。

5 打开光缆或 DSL 调制解调器的电源。

6 当电源适配器正确连接，电源指示灯会很快变成绿色。电源 LED 灯闪了几秒，当自检完成后指示灯停止闪动。如果闪动时间达一分钟或更长，请查阅“附录 A：常见问题解答”

7 打开连接到路由器上计算机的电源

无线连接到一台计算机

如果你想用无线连接接入路由器，按照以下步骤操作：

1 开启路由器前，确认酥油网络设备均断电，包括路由器，计算机，和光缆或 DSL 调制解调器。

2 从光缆或 DSL 调制解调器上把以太网的网络线与路由器控制面板上的互联网端口相连（见图 4-2）。这是唯一和你的调制解调器连接有效端口。

3 打开光缆或 DSL 调制解调器的电源

4 把电源适配器与电源端口连接（见图 4-3），并且把电源插头插入电源插座。

图 4-1

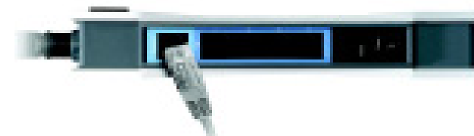


图 4-2

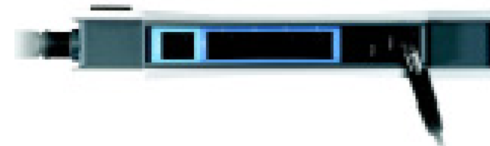
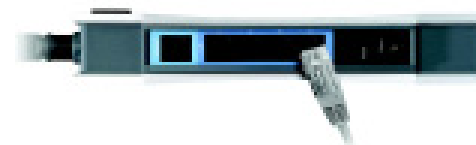
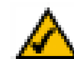


图 4-3





注释：你把路由器电源适配器插头插入插座时注意要用电源保护器。



注释：你应该经常改变从默认设置和 LINKSYS 的 SSID 身份识别码，以及激活 WEP 的加密功能。

- 一旦电源适配器正确连接，前面板上的 LED 电源指示灯会立刻亮启。电源指示灯会闪动几秒，自检结束后指示灯停止闪动。如果 LED 指示灯闪动一分钟或更长，查阅“附录 A：常见问题解答”

5 在你的无线网络上打开其中的一台计算机电源。

6 对于初次接入路由器的的无线网络连接，确认计算机的无线适配器有 SSID 识别设置到 LINKSYS-G（路由器的默认设置），确认 WEP 加密失效。接入路由器之后，你可以改变路由器和计算机适配器设置，去配合网络的常规设置。

路由器的硬件安装已完成。

进入“第五章：对计算机进行系统配置”

第五章：计算机的系统配置

综述

这一章里的指导帮助你如何对你的计算机进行配置，使计算机能与路由器交互。

为了达到此目的，你必须对计算机网络设置进行设定以自动获得 IP 地址或 TCP/IP 地址，由此你的计算机扮演 DHCP 客户端的功能。计算机用 IP 地址与路由器进行交互并且彼此穿过网络例如互联网。

首先，了解你的计算机所使用的操作系统。你可以点击开始菜单，打开资源管理器找出你的计算机所运行的操作系统。

你可以照此方法找出连接在路由器上其他计算机端的操作系统。

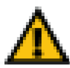
以下几页就告诉你如何一步步在不同的操作系统下进行网络设置。确认一个以太网或无线适配器（也可以称做网络适配器）已经在你要设置的计算机上成功安装。一旦你成功对你的计算机进行设置，请继续参阅“第六章：路由器基于网络的运用”。

对 WINDOWS 98 进行参数设置

1 点击开始菜单，选设置，点控制面板符号，双击网络标识。

2 在设置标签上，为使用中的以太网适配器选择 TCP/IP 协议，如图 5-1 所示。不要选择名为 DUN，PPPOE，VPN 或 AOL 的 TCP/IP 接入协议。如果 TCP/IP 单一显示，选择该项目。点击属性键。

3 点击 IP 地址标签。选择自动获得 IP 地址。（见图 5-2）



重要提示：WINDOWS 98，2000，ME 和 XP 已经安装了 TCP/IP，默认设置就是自动获得 IP 地址。如果你的计算机没有安装 TCP/IP 传输协议，点击开始菜单然后点帮助。寻找 TCP/IP 的关键字。然后根据以下提示安装 TCP/IP 协议。

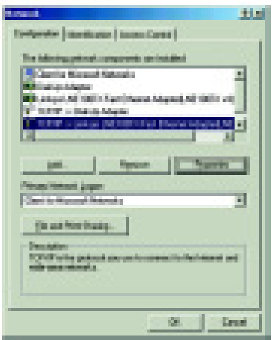


图 5-1：设置标签



图 5-2：地址标签

4 点击 GATEWAY 标签，确认 GATEWAY 字段为空。点击 OK 键

5 再次点击 OK 键。WINDOWS 会问你要 WINDOWS 安装原盘或额外文件。确认文件的路径是 C:\Windows\options\cabs,或插入你的 WINDOWS 安装盘到光驱里,并确认文件位置等。D:\WIN98, D:\WIN9X 等（如果盘符“D”是你的光盘驱动器符号)。

6 完成后，WINDOWS 系统问你是否需要重新启动你的计算机，点击“是”，如果 WINDOWS 系统没有问你是否要重新启动，你也重新启动。

详见“第六章：使用路由器的网络功能”

对 WINDOWS 2000 操作系统的计算机进行网络设置

1 点击“开始”菜单键。选择设置并点击控制面板。双击网络和拨号上网。

2 为所使用以太网适配器选择局域网（本地连接）符号。双击局域网，打开属性。（见图 5-3）

3 确认 TCP/IP 的互联网协议。选中互联网协议（TCP/IP），点击属性键（图 5-3）

4 选择自动获得 IP 地址。一旦新的窗口出现，点击“OK”键。再次点击 OK 键完成计算机参数设置。（见图 5-53）

5 重新启动计算机

详见“第六章：路由器在网络上的运用”

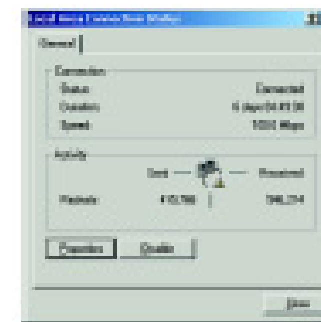


图 5-3：属性

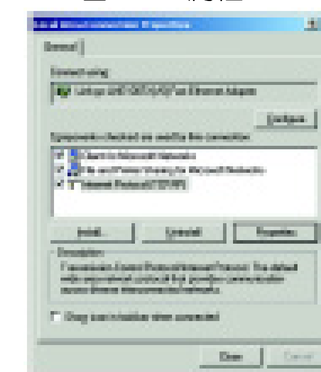


图 5-4：TCP/IP

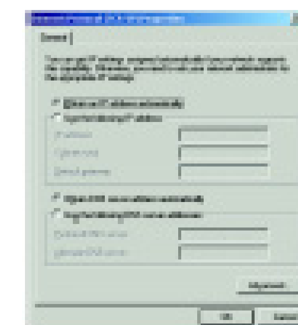


图 5-5：IP 地址

对 WINDOWS XP 操作系统的计算机参数设置

接下来的指导假定你用默认属性界面运行 WINDOWS XP。如果你在用老式的界面(看上去好象以前的 WINDOWS 操作系统版本)，请按以下指导来操作：

1 点击开始菜单，然后点控制面板。点击网络和互联网连接，再点击网络连接标识。

2 选择局域网（本地连接）标识，双击局域网连接，点击属性。（见图 5-6）

3 确认互联网协议（TCP/IP)。选互联网协议（TCP/IP)，并点击属性按钮。（见图 5-7）

4 选择自动获得 IP 地址。（见图 5-8)。一旦新的窗口出现，点击 OK。再次点击 OK 完成整个计算机的参数设置。

参阅“第六章；路由器基于网络的应用”

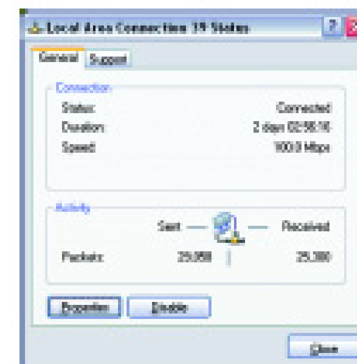


图 5-6：属性

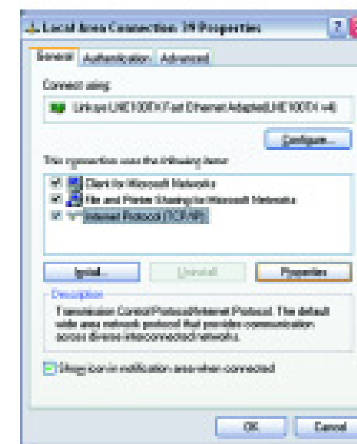


图 5-7：TCP/IP

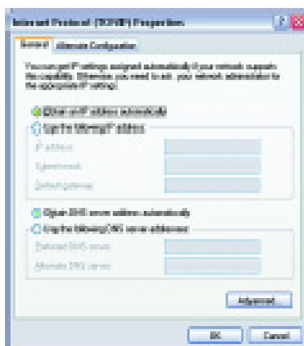


图 5-8：IP 地址

第 6 章　配置路由器

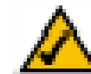
综述

Linksys 建议第一次安装路由器和另安装一台计算机时使用 CD-ROM 安装软件。如果你不希望在 CD-ROM 安装软件上运行安装向导，那么你按本章步骤并利用路由器以网络为基础的实用程序配置路由器。本章将描述实用程序中的每一个网页和每一网页的关键功能。此实用程序可通过使用连到路由器上的计算机经由你的网页浏览器而进行使用。有关基本网络安装，大多数用户仅得使用下列实用程序屏:

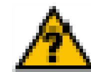
- 基本安装。在基本安装屏上，输入你的 ISP 提供的设置。

- 管理。点击**管辖**标签，接着**管理**标签。路由器的默认密码是 admin。为了保证路由器，从其默认密码来改变。

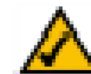
有七个主标签: 安装、无线、安全、访问限制、应用程序及对策、管辖和状态。你点击主标签中的一个，另一标签将有效。



注意: 路由器用于把路由器连到你的网络后起到正确运行作用。本章仅针对于想要执行更高级的人。



你已启动了你的个人计算机上的 TCP/IP 地址了吗？用此协议通过网络的个人计算机通信，参照附录 D: 有关 TCP/IP 的更多信息的 Windows 帮助。



注意: 有关已添加的安全，你应通过以网络基础的实用程序的管辖屏改变密码。

安装

- 基本安装。在本屏上输入互联网连接和网络设置。
- DDNS。启动路由器的动态域名系统 (DDNS)，在本屏上填写字段。
- MAC 地址克隆。如你需要把 MAC 地址克隆在路由器上，使用本屏。
- 高级路由器选择。在本屏上，你可以改变网络地址转换 (NAT)、动态路由器选择和动态路由器选择配置。
- 热点。用你的热点服务供应商在本屏上注册。

NAT (网络地址转换): NAT 技术把本地区域网络的 IP 地址换成互联网的不同 IP 地址。

无线

- 基本无线设置。你可以在本屏上选择你的无线网络型号和无线安全。
- 无线网络访问。本屏显示你的网络访问表。

● 高级无线设置。在此屏上，你可以访问高级无线验证类型、基本数据率、控制 Tx 率、信标间隔、DTIM 间隔、RTS 阀值和分段阀值的性能。

安全

● 过滤器。阻止指定用户访问互联网，你可以安装过滤器屏过滤的 IP 地址、端口和 MAC 地址。
● VPN。启动或停止 IPSec，L2TP 和/或 PPTP 浏览并安装 VPN 通道，请使用此屏。
● 802.1x。使用此屏安装 RADIUS 验证。

访问限制

● 访问限制。此屏仅使你能防止或许可某些用户连到你的网络上。

应用程序及对策

● 端口距离发送。在你的网络上安装公共服务或其它专门互联网应用程序，点击此标签。
● 端口触发。安装互联网应用程序的触发距离和发送距离，点击此标签。
● UP$_n$P 发送。使用此屏改变 UP$_n$P 发送设置。
● DMZ。允许一个本地用户访问互联网使用专门目的服务，使用本屏。

管辖

● 管理。在本屏上改变你的路由器访问特权和 UP$_n$P 设置。
● 记录。如果你想浏览或保存活动记录，点击此标签。
● 诊断。使用此屏检查你的路由器和个人计算机之间的连接。
● 工厂默认。如果你想恢复路由器的工厂默认，那么使用此屏。
● 固件升级。如果你想升级路由器的固件，点击此标签。

信标间隔：信标的经常间隔，它是由使无线网络同步的路由器发出的数据包广播。

DTIM（发送交通识别信息）：能增加无线效率的数据包中含有的一个信息。

RTS（请求发送）：一个当计算机有数据传送时发送包。计算机将在发送数据以前等待一个 CTS（清除发送）信息。

分段：当通过一个不能支付原包大小的网络媒介传送时，把数据包插入一个较小的装置里。

状态

- 路由器。此屏提供有关路由器的状态信息。
- 局域网络。此屏提供有关局域网络的状态信息。

如何访问以网络为基础的实用程序

访问以网络为基础的实用程序，启动互联网资源管理器或 Netscape 导航器，并在地址段里输入路由器的默认 IP 地址 192168.1.1。接着按输入。

6-1 图所示的密码请求页将出现。（非 Windows XP 用户将看见类似的屏幕。）
在用户名字段里输入 admin（用户默认姓名），并在密码字段里输入 admin（默认密码），接着点击 OK 按钮。

安装标签

基本安装标签

显现的第一屏是基本安装标签。（见 6-2 图）此标签使你能改变路由器的一般设置。改变此处所述的这些设置，点击**保存设置**按钮保存你的改变或点击**取消改变**按钮取消你的改变。

互联网安装

- 互联网连接类型。路由器支持四个连接类型：自动配置 – DHCP（默认连接类型）、PPPoE、固定 IP 和 PPTP。每个基本安装屏和现有性能取决于你选择的哪种连接类型而不同。

自动配置 – DHCP

把路由器的配置类型默认设为自动配置 – DHCP，如果你的 ISP 支付 DHCP 或你在通过一个动态 IP 地址连接时，仅保持它。



6-1 图:密码屏



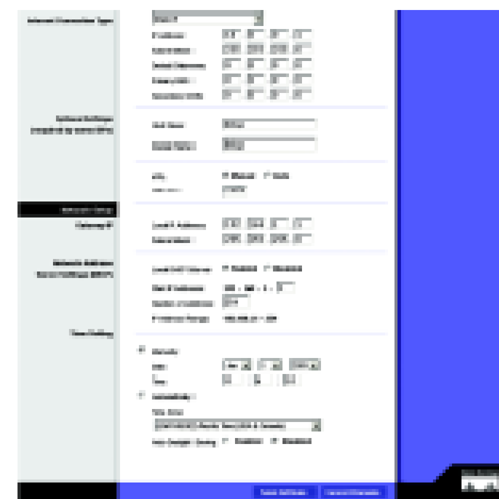
6-2 图:安装标签/DHCP 互联网连接类型

固定（见 6-3 图）

如果要求你使用永久 IP 地址连接到互联网，那么选择固定 IP。

- IP 地址：这是 WAN 或互联网上出现的路由器 IP 地址，此处你的 ISP 将向你提供你需要说明的 IP 地址。
- 子网掩码。这是由互联网外部用户所见的路由器子网掩码（含你的 ISP）。你的 ISP 将向你提供子网掩码。
- 默认网关。你的 ISP 将向你提供默认网关地址，它是 ISP 服务器的 IP 地址。
- 初级 DNS。（规定的）和二级 DSN（任选的）。你的 ISP 将向你提供至少一个 DNS（域名系统）服务器 IP 地址。

当在标签上改完后，点击**保存设置**按钮保存这些改变或点击**取消改变**按钮取消你的改变。



6-3 图:固定互联网连接类型

PPPoE（见 6-4 图）

一些基于 DSL 的 ISPs 使用 PPPOE（通过 Ethernet 的点对点协议）建立互联网连接。如果通过 DSL 线连到互联网，用你的 ISP 检查看是否他们使用 PPPoE，如果你在使用，你将必须启动 PPPoE。

- 用户名和密码。输入你的 ISP 提供的用户名和密码。
- 一经要求连接：最大空闲时间。路由器在指定时间内（最大空闲时间）停用后，你可配置它断开互联网连接。如果你的互联网连接由于停用已停止，一旦你要再次访问互联网，一经要求连接就启动路由器自动重新建立你的连接。如果你想激活**一经要求连接**，点击单选按钮。在最大空闲字段里，输入你想要在你的互联网连接终止以前流逝的时间数字。
- 保持有效选项：重拨期。如果你选择此选项，路由器将定期检查你的互联网 连接。如果你已断开，那么路由器将自动重新建立你的连接。使用此选项，点击单选按钮到**保持有效**。在重拨期字段里，你指定你想要路由器多长时间检查互联网连接。默认重拨是 30 秒。

当在此标签上改完后，点击**保存设置**按钮保存这些改变或点击**取消改变**按钮取消你的改变。



6-4 图:PPPoE 互联网连接类型

PPTP（见 6-5 图）

点对点通道协议（PPTP）是仅应用于在欧洲连接的一项服务（见 6-8 图）。

●互联网 IP 地址。这是在互联网上看见的路由器的 IP 地址，此处你的 ISP 将向你提供你需要说明的 IP 地址。
●子网掩码。这是由互联网外部用户所见的路由器子网掩码（含你的 ISP）。你的 ISP 将向你提供子网掩码。
●默认网关。你的 ISP 将向你提供默认网关地址。
●用户名和密码。输入你的 ISP 提供的用户名和密码。
●一经要求连接：最大空闲时间。路由器在指定时间内（最大空闲时间）停用后，你可配置它断开互联网连接。如果你的互联网连接由于停用已停止，一旦你要再次访问互联网，一经要求连接就启动路由器自动重新建立你的连接。如果你想激活**一经要求连接**，点击单选按钮。在最大空闲字段里，输入你想要在你的互联网连接终止以前流逝的时间数字。
●保持有效选项：重拨期。如果你选择此选项，路由器将定期检查你的互联网 连接。如果你已断开，那么路由器将自动重新建立你的连接。使用此选项，点击单选按钮到**保持有效**。在重拨期字段里，你指定你想要路由器多长时间检查互联网连接。默认重拨是 30 秒。

当在此标签上改完后，点击**保存设置**按钮保存这些改变或点击**取消改变**按钮取消你的改变。

任选设置（一些 ISP 所要求的）

●主机名和域名。这些字段使你能为路由器提供主机名和域名。一些 ISPs 要求这些名称作为标识。你必须用你的 ISP 检查看你的宽带互联网服务是否已配有主机名和域名。大多数情况下，这些字段留有空白仍将运行。

●MTU。MTU（最大传输单元）设置指定网络传送许可的最大包大小。选择**启动**并输入想要的值。建议你在 1200 至 1500 范围内设值。对大多数 DSL 用户，建议使用 1492 值。MTU 当无效时，默认为在 1500 值。



6-5 图：PPTP 互联网连接类型

- 网关 IP。此处所示的是路由器的本地 IP 地址和子网掩码的值。大多数情况下，保持默认值将运行。

- 本地 IP 地址。默认值是 192.168.1.1。

- 子网掩码。默认值是 255.255.255.0。

- 网络地址服务器设置（DHCP)。动态主机配置协议（DHCP）服务器自动向你的网络上的每台个人计算机分配一个 IP 地址。除非你已经有一个，强烈建议你把启动的路由器留作一个 DHCP 服务器。
本地 DHCP 服务器。DHCP 由工厂默认启动。如果在你的网络上你已一个 DHCP 服务器，把路由器 DHCP 选项设为停止。如果你停止 DHCP，记住向路由器分配一个固定 IP 地址。

- 启动 IP 地址。输入 DHCP 服务器的一个值以从发出 IP 地址时启动。此值必须是 192.168.1.2.

- 地址数。输入你想要 DHCP 服务器把 IP 地址分配给个人计算机的最多数。此数不能大于 253。向 DHCP 用户数确定 DHCP IP 地址范围和启动 IP 地址（例如 100)，按 6-9 图所示，100 加 50 的默认范围是 192.168.1.1.00 到 192.168.1.149。

- DHCP 地址范围。此处所示的是 DHCP 地址范围。

- 时间设置。你是你为你的路由器设置时间的地方。你可通过设置时间区手动或自动设置时间和数据。

当在此标签上改完后，点击**保存设置**按钮保存这些改变或点击**取消改变**按钮取消你的改变。

DDNS 标签

路由器提供一个动态域名系统（DDNS）性能。DDNS 使你能向一个动态互联网 IP 地址分配一个固定主机名和域名。当你在自己的网址、FTP 服务器或路由器后面的其它服务器时，它是有用的。

在你能使用此性能以前，你需要在两个 DDNS 服务供应商之一上签订 DDNS 服务、DynDNS.org 或 TZO.org.。

DDNS

DDNS 服务。如果你的 DDNS 服务是由 DynDNS.org.提供，那么选择下拉框菜单里的 DynDNS.org。（见 6-6 图）。如果你的 DDNS 服务是由 TZO 提供，那么选择 TZO。（见 6-7 图）DDNS 屏上现有的性能取决于你使用的哪个 DDNS 服务供应而不同。



6-6 图：DynDNS.org

DynDNS.org

- 用户名、密码和主机名。输入你用 DynDNS.org.安装的帐户的用户名、密码和主机名。
- 互联网 IP 地址。此处显示的是路由器的当前互联网 IP 地址。因为它是动态的，将有所改变。
- 状态。此处所显示的是 DDNS 服务连接的状态。

当在此标签上改完后，点击**保存设置**按钮保存这些改变或点击**取消改变**按钮取消你的改变。



6-7 图：TZO.com

TZO.com 标签

- 电子邮件地址、TZO 密码键和域名。输入你用 TZO 安装的服务的电子邮件地址、TZO 密码键和域名。
- 互联网 IP 地址。此处显示的是路由器的当前互联网 IP 地址。因为它是动态的，将有所改变。
- 状态。此处显示的是 DDNS 服务连接状态。

当在此标签上改完后，点击**保存设置**按钮保存这些改变或点击**取消改变**按钮取消你的改变。

MAC 地址克隆标签（见 6-8 图）

路由器的 MAC 地址是一个分配给唯一一个标识硬件像社保号码一样的 12 位代码。如果你的 ISP 要求 MAC 地址注册，按附录 D：查找你的 Ethernet 适配器的 MAC 地址和 IP 地址中说明查找你的适配器的 MAC 地址。



6-8 图：MAC 地址克隆

MAC 克隆

- MAC 克隆服务。使用 MAC 地址克隆法，选择**启动**。
- MAC 地址。手动克隆 MAC 地址，在屏上字段输入你的适配器 MAC 地址的 12 位数。（见 6-2 图），接着点击**保存设置**按钮。
- 克隆我的 MAC 地址。如果你想要克隆你目前正在使用的个人计算机的 MAC 地址配置路由器，那么点击**克隆我的 MAC 地址**按钮。路由器将自动检测你的个人计算机的 MAC 地址，你不要调你的 ISP 把已注册的 MAC 地址改到路由器的 MAC 地址。建议用 ISP 注册的个人计算机用于打开 MAC 地址克隆标签。

当在此标签上改完后，点击**保存设置**按钮保存这些改变或点击**取消改变**按钮取消你的改变。

高级路由器标签

高级路由器标签允许你配置动态路由选择和固定路由选择设置。（见 6-9 图）



6-9 图：高级路由选择

高级路由器

- 运行模式。从下拉菜单中选择运行模式的**网关或路由器。**
- 动态路由选择。用动态路由选择，你可以启动路由器自动适应网络布置的物理改变。路由器使用 RIP 协议确定基于资源与目的地之间少数站段的网络包路由。RIP 协议定期向网络上的其它路由器广播路由选择信息。
- 接收 RIP 版本。使用动态路由选择接收网络数据，选择你想要的协议：RIP1 或 RIP2。
- 传送 RIP 版本。使用动态路由选择传送网络数据，选择你想要的协议：RIP1、RIP1-兼容或 RIP2。

固定路由选择

如果路由器连到一个以上的网络，在它们之间安装固定路由是必须的。固定路由是一个网络信息到达指定主机或网络的预先确定的路径。创造一个固定路由，改变下列设置：

●选择号码。从下拉菜单中选择固定路由的**号码**。路由器支持最多 20 个固定路由条目。

●删除条目。如果你需要删除路由，从下拉菜单中选择其号码，并点击**删除条目**按钮。

●局域网 IP 地址。局域网 IP 地址是你要把固定路由分配到远程网络或主机的地址，输入你想创建一个固定路由的主机 IP 地址。如果你正在为整个网络建立一个路由，确保 IP 地址的网络部分设为 0。例如：路由器的标准 IP 地址是 192.168.1.1。基于此地址，已发送网络的地址是 192.168.1，用最后数字确定路由器在网络上的位置。所以如果你要发送到路由器的整个网络而不仅是给路由器，你应输入 IP 地址 192.168.1.0。

●子网掩码。子网掩码（又称网络屏蔽）确定一个 IP 地址的哪部分是网络部分，哪部分是主机部分。以子网掩码是 255.255.255.0 的网络为例，这确定（通过使用 255 值）网络 IP 地址的前三位数确定特定的网络，而末位数（从 1 至 254）确定指定的主机。

●默认网关。此 IP 地址应是考虑到路由器和远程网络或主机间联系的网关装置的 IP 地址。

●米制。这确定数据包将到的网络节点间的最大步进数。节点是网络上的任何装置，如个人计算机、打印服务器、路由器等。

●接口。选择**局域网**及**无线**或**互联网**，取决于固定路由器最终目的地的位置。

●显示路由选择标签。点击**显示路由选择标签**打开显示通过你的**局域网**发送多少数据的屏面。有关每个路由，显示目的地局域网 IP 地址、子网掩码、默认网关和接口。点击**刷新**按钮升级信息。见 6-10 图。

当在此标签上改完后，点击**保存设置**按钮保存这些改变或点击**取消改变**按钮取消你的改变。



6-10 图：路由选择标签

无线标签

基本无线设置（见 6-11 图）

此屏使你能选择无线网络模式和无线安全。

无线网络

● 无线网络模式。如果你有网络的无线-G 和 802.11b 装置，那么保持默认设置**混和**。如果仅有无线-G 装置，选择**唯一的** G。如果你要停止无线网络，选择**停止**。

● 无线网络名。在字段里输入**无线网络名（SSID）**。SSID 是在无线网络中的所有装置共享的网络名，SSID 必须对无线网络中的所有装置是一样的。它是区分大小写并且不得超过 32 位字母数字字符，字符可以是任何键盘字符。有关添加安全，Linksys 建议你把默认 SSID（linksys）改成一个你选择的唯一名。

● 无线通道。从提供符合你的网络设置的表单中选择相应的通道，1 和 11 之间（北美洲）。你的无线网络的所有装置必须使用同一通道以便正确运行。



6-11 图：基本无线

无线安全

●无线 SSID 广播。当无线客户调查相关的无线网络的局部区域时，他们将通过路由器检测 SSID 广播。广播路由器的 SSID，保持默认设置**启动**。如果你不要广播路由器的 SSID，那么选择**停止**。

●WEP。有线等效保密的缩写字母。WEP 是一个用于保护你的无线数据通信的加密方法。WEP 使用 64 位或 128 位键向你的网络和每个数据传送的加密安全提供访问控制。为了译解数据传送，所有网络中的无线-G 装置和 802.11b 必须使用同一 WEP 键。高级加密级别提供更高的安全级别，但由于加密的复杂性，他们可以降低网络性能。启动 WEP 加密，点击**启动**广播按钮，接着点击**编辑 WEP 设置**按钮配置 WEP 设置。停止 WEP 加密，保持默认设置**停止**。

WEP（见 6-12 图）

WEP 允许你配置 WEP 设置。应始终启动 WEP 加密增加你的无线网络安全。默认传送键。当路由器发送数据时，选择将使用的 WEP 键（1-4）。确保接收装置在使用同一个键。

●WEP 加密。选择你想使用的 WEP 加密级别：64-位 10 个十六进制数字或 128-位 26 个十六进制数字。高级加密级别提供更高的安全级别，但由于加密的复杂性，它们可以降低网络性能。
●Passphrase。不用手动输入 WEP 键，你可以输入 Passphrase。此 Passphrase 用于产生一个或多个 WEP 键。它是区分大小写并且不应大于 16 位字母数字字符。（此 Passphrase 性能仅兼容 Linksys 无线产品。如果你要与非 Linksys 无线产品通信，在非 Linksys 无线产品上手动输入 WEP 键。）你输入 Passphrase 后，点击**产生**按钮创建 WEP 键。
● 键 1-4。WEP 键使你能创建一个无线局域网传送的加密方案。如果你不在使用一个 Passphrase，那么手动输入一套值。（不要留键字段空白，并且不要输入所有的零，这些是无效的键值。）

如果你在使用 64-位 WEP 加密，那么此键必须是正确的 10 个十六进制数字字符长度。如果你在使用 128-位 WEP 加密，那么此键必须是正确的 26 个十六进制数字字符长度。有效的十六进制数字字符是“0”至“9”和“A”至“F”。

当在此标签上改完后，点击**保存设置**按钮保存这些改变或点击**取消改变**按钮取消你的改变。



6-12 图：WEP

无线网络访问（见 6-13 图）

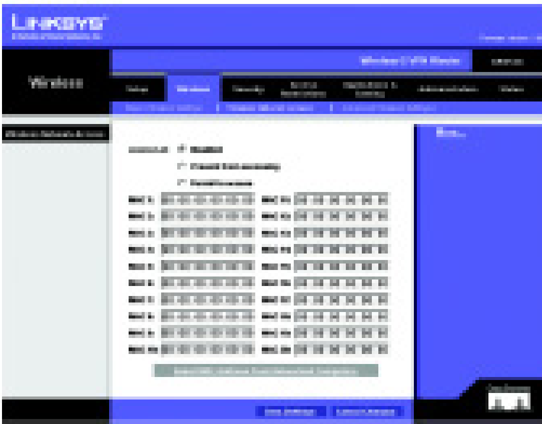
无线网络访问。如果此功能启动，仅允许表单上的计算机访问无线网络。给网络添加计算机，点击**许可访问**按钮并在字段里输入 MAC 地址。点击**从联网计算机上选择 MAC 地址**按钮，6-15 图上的屏面将显现。

从表单上选择 **MAC 地址**并点击**选择**按钮。

防止访问，点击**防止访问**按钮，接着点击**从表单上选择 MAC 地址**，从 6-14 图上的屏面选择表单中的 **MAC 地址**，并点击**选择**按钮。

如果你要刷新屏面，点击**刷新**按钮。点击**关闭**按钮返至原先的屏面。

当在此标签上改完后，点击**保存设置**按钮保存这些改变或点击**取消改变**按钮取消你的改变。



6-13 图：无线网络访问



6-14 图：联网计算机

高级无线设置（见 6-15 图）

在此屏上你可访问包括验证类型、基本数据率、控制 Tx 率、信标间隔、DTIM 间隔、RTS 阀值和分段阀值的高级无线性能。

●验证类型。默认设为自动，这允许使用打开系统或共享键验证。有关打开系统验证，发送人和接收人不要用 WEP 键进行验证。有关共享键验证，发送人和接收人使用 WEP 键进行验证。如果你仅要使用共享键验证，那么选择**共享键**。

●基本数据率。从下拉菜单中选择 1-2Mbps、**所有或默认。**

●控制 Tx 率。默认传送率是自动的。范围从 1 至 54Mvps。设置数据传送率取决于你的无线网络的速度，你能从传送速度范围中选择或保持默认设置-自动，让路由器自动使用可能最快的数据率并启动自动低效性能。自动低效将协商路由器与无线客户间的最佳连接速度。

●信标间隔。默认值是 100。输入 1 至 65,535 毫秒间的值，信标间隔指示信标的经常间隔。信标是一个由路由器发出的包广播以使无线网络同步。

●DTIM 间隔。默认值是 3。在 1 至 255 毫秒间的值指示发送交通指示信息（DTIM）的间隔。DTIM 字段是一个通知客户收听广播和多点发送信息的下一个窗口的倒计时字段。当路由器为相关客户缓冲广播或多点发送信息时，它用 DTIM 间隔值发送下一个 DTIM，它的客户听到间隔并唤醒接收广播和多点发送信息。

●RTS 阀值。此值应保持在 2347 的默认设置，范围是 0 至 2347 字节。如果你遇到不一致的数据流，仅建议较小的修改。如果网络包比预设的 RTS 阀值尺寸小，RTS/CTS 机制将不能被启动。路由器向特定的接收站发送请求发送（RTS）帧并协商数据帧的发送。收到一个 RTS 后，无线站用清除发送（CTS）响应以确认开始传送的权利。

●分段阀值。。此值应保持在 2346 的默认设置，范围是 256 至 2346 字节。数据分成多个包以前，它指定一个包的最大尺寸。如果你体验一个高包错误率，你可以略微增加分段阀值，设置分段阀值太低可导致差误的网络性能。仅建议较小的修改。



6-15 图：高级无线设置

安全标签

防火墙



6-16 图：防火墙

当你点击安全标签时，你将看见防火墙屏（6-16 图）。此屏含有过滤器和 WAN 块请求。过滤器阻止指定用户访问互联网并阻止匿名互联网请求和/或多点发送。

●防火墙。添加防火墙保护，点击**启动**。如果你不要防火墙保护，点击**停止**。

●过滤器代理。使用 WAN 代理服务器可危及路由器的安全。否认过滤器代理将停止访问任何 WAN 代理服务器。启动代理过滤器，点击**启动**。

●Cookie 过滤器。Cookie 是当你与它们相互作用时，你的个人计算机上存储并由互联网站点使用的数据。启动 Cookie 过滤，点击**启动**。

●Java Applets 过滤器。Java 是网站的程序设计语言。如果你否认 Java Applets，你有不访问使用此程序设计语言创建的互联网站点的风险。启动 Java Applet 过滤，点击**启动**。

●ActiveX 过滤器。ActiveX 是网站的程序设计语言。如果你否认 ActiveX，你有不访问使用此程序设计语言创建的互联网站点的风险。启动 ActiveX 过滤，点击**启动**。

●多点发送过滤器。多点发送允许同时向指定的接收人多点传送。如果多点发送得到许可，路由器将允许 IP 多点发送包被寄发给相应的计算机。启动多点过滤器，选择**启动**，停止此性能，选择**停止**。

●阻止匿名互联网请求。这可防止你的网络发出脉冲信号或被检测到并通过隐藏你的网络端口加强你的网络安全，所以入侵者很难插入你的网络。选择**启动**阻止匿名互联网请求，或选择**停止**允许匿名互联网请求。

当在此标签上改完后，点击**保存设置**按钮保存这些改变或点击**取消改变**按钮取消你的改变。

VPN

虚拟专用网络（VPN）是在远程两地间创建一个安全连接的安全措施，就有关它的设置，此连接是非常特殊的，这是创建安全所需的。6-17 所示的 VPN 屏允许你配置你的 VPN 设置以使你的网络更安全。

VPN Pass Through（虚拟专用网络浏览）

●IPSec Passthrough。互联网协议安全（IPSec）是一套用于执行 IP 层上包的安全交换的协议。允许 IPSec Passthrough，点击**启动**按钮，停止 IPSec Passthrough，点击**停止**按钮。

●PPTP Pass Through（PPTP 游览）。点对点通道协议 Passthrough 是用于启动通向 Windows NT 4.0 或 2000 服务器的 **VPN** 对话。允许 PPTP Passthrough，点击**启动**按钮。停止 PPTP Passthrough，点击**停止**按钮。

●L2TP Pass Through（L2TP 游览）。2 层通道协议 Passthrough 是通过互联网启动 Virtual 保密网络（VPN）运行所用的点对点通道协议（PPTP）的扩展。允许 L2TP Passthrough，点击**启动**按钮，停止 L2TP Passthrough，点击**停止**按钮。

VPN 通道

VPN 路由器在两个端点之间创建一个通道，以便这两个端点间的数据或信息是安全的。

●建立此通道，在选择通道条目下拉框中选择你想创建的通道，可同时创建 50 个通道，接着点击**启动**以启动通道。一旦通道启动，在通道名称字段里输入通道名称，这样可允许你确认多个通道并且不必匹配通道另一端使用的名称。

●本地安全集团及远程安全集团。本地安全集团是在你的可访问通道的局域网上的计算机。远程安全集团是在可访问通道的通道远程末端上的计算机。在字段里输入本地 VPN 路由器的 **IP 地址及子网掩码**。允许访问整个 IP 子网，在 IP 地址的最末位输入 0。（例如：192.168.1.0）.

●远程安全网关。远程安全网关是 VPN 通道远程末端上的如第二个 VPN 路由器的 VPN 地址。在通道的另一端输入 VPN 装置的 IP 地址，远程 VPN 装置可以是另一个 VPN 路由器、VPN 服务器或一个有支持 IPSec 的 VPN 客户软件的计算机。IP 地址可以是固定（永久）或动态（变换），这取决于远程 VPN 装置的设置。确保你已正确地输入 IP 地址或不作改正。记住，这不是本地 VPN 路由器的 IP 地址，而是你想联系的远程 VPN 路由器或装置的 IP 地址。



6-17 图：VPN

● 加密。使用加密也帮助你更安全的连接。有两种不同类型的加密：DES 或 3DES（建议 3DES，因它更安全）。你可选择任一一个，但它必须是由通道另一端上的 VPN 装置所在使用的同一类型的加密，或者通过选择停止，选择不加密。6-18 图已选择 DES（默认）。

● 验证。验证充当另一级的别安全。有两种类型的验证：MD5 和 SHA（建议 SHA，因为它更安全）。如用加密，只要通道另一端上的 VPN 装置在使用同一种类型的验证，可以选择这两种类型的任一一种，或者通道两端选择停止验证。6-18 图已选择 MD5（默认）。

● 键管理。键交换方法。使用键交换方法，选择**自动**（IKE）或**手动**。以下描述两种方法：

自动（IKE）

选择**自动**（IKE）并在预共享键字段里输入序列号，检查 PFS（完全正向保密）旁的框以确保最初键交换和 IKE 协议是安全的，基于此话，如果使用此方法，必须在通道的两端输入，键产生以加密通过未被加密的通道传送的数据。你可在此字段里混和输入最多 24 个数或字母，不允许特殊的字符或空格。在键使用期限字段里，你可随意选择让键在你所选择的时间期末终止，输入你想要键有用的秒数或在字段上无限期地持续留键空白。

手动（见 6-18 图）

选择**手动**，接着在下拉菜单中选择加密算法，在字段里输入加密键（对于加密算法，如果你选择 DES，输入 16 个十六进制字符。如果你选择 3DES，输入 48 个十六制字符。）。从下拉菜单中选择验证算法，在字段里输入验证键（对于验证算法，如果你选择 MD5，输入 32 个十六进制字符。如果你选择 SHA1，输入 40 个十六制字符。）。在各自的字段里输入入站和出站 SPIs。

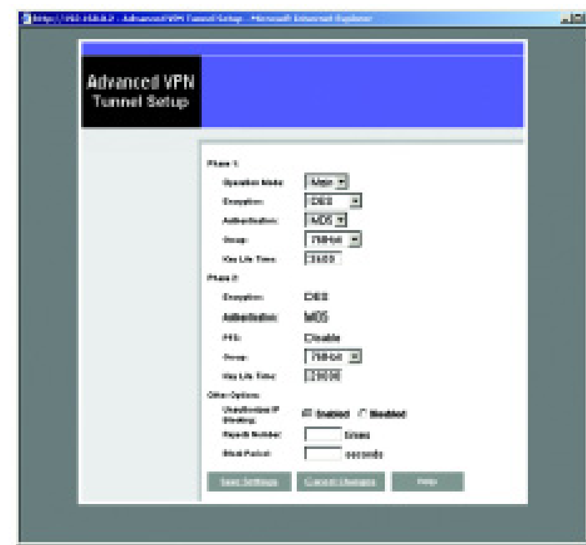
● 状态。点击**高级 VPN 通道安装**键，高级 VPN 通道安装屏将出现。
见 6-20 图。



6-18 图：手动键管理

当在此标签上改完后，点击**保存设置**按钮保存这些改变或点击**取消改变**按钮取消你的改变。高级 VPN 通道安装

从 6-19 图所示的高级 VPN 通道安装屏，你可调整指定的 VPN 通道的设置。



6-19 图：高级 VPN 通道安装

第 1 阶段

●第 1 阶段用于创建安全联系（SA），经常称作 IKE SA。完成第 1 阶段后，第 2 阶段用于创建一个或多个 IPSec SAs，它用于键 IP Sec 会话。
●运行模式。有两种模式：主要和主动，并且他在不同的顺序里交换同一 IKE 有效荷载。主要模式更通用，然而一些人更喜欢主动模式，因为它更快。主要模式用于正常使用并含有比主动模式多的验证要求。建议使用主要模式，因为它更安全。不管选择哪种模式，VPN 路由器都接受远程 VPN 装置发出的主要和主动请求。
●加密。选择用于加密/解密 ESP 包的键长度。有两种选择：DES 和 3DES。建议用 3DES，因为它更安全。
●验证。选择用于验证 ESP 包的方法。有两种选择：MD5 和 SHA。建议用 SHA，因为它更安全。
●集团。有两个供选择的 Diffie-Hellman 集团：768-位和 1024-位。Diffie-Hellman 指使用加密及解密的公共和专用键的密码技术。
●键使用期限。在键使用期限字段里，你可随意选择让键在你所选择的时间期末终止。在完成每个端点间的重-键协商以前输入你想要键有用的秒数。

第 2 阶段

●加密。第 1 阶段所选择的加密方法将被显示。
●验证。第 1 阶段所选择的验证方法将被显示。
●集团。有两个供选择的 Diffie-Hellman 集团：768-位和 1024-位。Diffie-Hellman 指使用加密及解密的公共和专用键的密码技术。
●键使用期限。在键使用期限字段里，你可随意选择让键在你所选择的时间期末终止。在完成每个端点间的重-键协商以前输入你想要键有用的秒数。

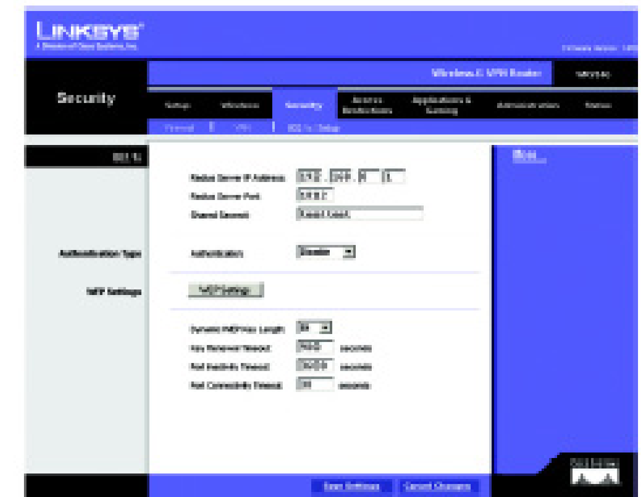
其它选项

● 未经授权的 IP 阻塞。点击**启动**阻塞未经授权的 IP 地址。在拒收号字段里输入说明在阻塞未经授权的 IP 地址以前 IKE 必须失效多长时间。输入你在阻塞期字段里说明的时间长度（用秒）。

当在此标签上改完后，点击**保存设置**按钮保存这些改变或点击**取消改变**按钮取消你的改变。
有关此标签的进一步帮助，点击**帮助**按钮。

安全

802.1X（见 6-20 图）



6-20 图：802.1X

● 半径服务器 IP 地址。在字段里输入半径服务器 IP 地址。
● 半径服务器端口。在字段里输入半径服务器端口。
● 共享秘密。在字段里输入共享秘密。
●验证类型。启动 EAP-TLS，点击 EAP-TLS。启动 EAP-TTLS，点击 EAP-TTLS。启动 EAP-MD5，点击 **EAP-MD5**。停止验证，点击**停止**。
● WEP 设置。点击 **WEP 设置**按钮编辑设置，7-22 图将显现。
● 动态 WEP 键长度。大下拉菜单中选择 64 或 128 位。
● 键更新超时。用秒输入键更新时间。
● 端口静止超时。用秒输入端口静止时间。
● 端口连通超时。用秒输入端口连通时间。

当在此标签上改完后，点击**保存设置**按钮保存这些改变或点击**取消改变**按钮取消你的改变。

WEP

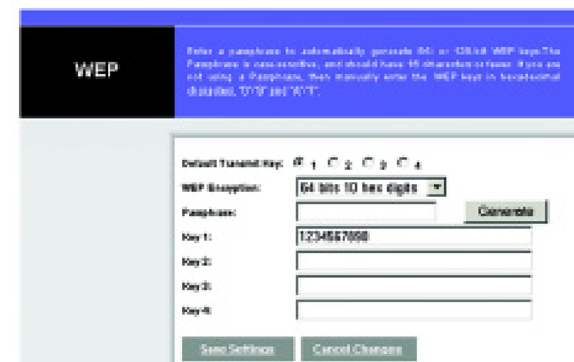
WEP 屏允许你配置你的 WEP 设置，（见 6-21 图。）应始终启动 WEP 加密以增加你的无线网络的安全。默认传送键。当路由器发送数据时，选择将使用的 WEP 键（1-4），确保接收装置在使用同一键。

●WEP 加密。选择你相使用的 WEP 加密级别：64-位 10 个十六进制数字或 128-位 26 个十六进制数字。高级加密级别提供更高的安全级别，但由于加密的复杂性，它们可降低网络性能。

●Passphrase。不用手动输入 WEP 键，你可以输入 Passphrase。此 Passphrase 用于产生一个或多个 WEP 键。它是区分大小写并且不应大于 16 位字母数字字符。（此 Passphrase 性能仅兼容 Linksys 无线产品。如果你要与非 Linksys 无线产品通信，在非 Linksys 无线产品上手动输入 WEP 键。）你输入 Passphrase 后，点击**产生**按钮创建 WEP 键。

● 键 1-4。WEP 键使你能创建一个无线局域网传送的加密方案。如果你不在使用一个 Passphrase，那么手动输入一套值。（不要留键字段空白，并且不要输入所有的零，这些是无效的键值。）

如果你在使用 64-位 WEP 加密，那么此键必须是正确的 10 个十六进制数字字符长度。如果你在使用 128-位 WEP 加密，那么此键必须是正确的 26 个十六进制数字字符长度。有效的十六进制数字字符是“0”至“9”和“A”至“F”。
当在此标签上改完后，点击**保存设置**按钮保存这些改变或点击**取消改变**按钮取消你的改变。



6-2 1 图：WEP

访问限制标签

访问限制

6-22 图所示的访问限制标签允许你阻塞或允许指定的互联网使用。你可以为指定的个人计算机安装互联网访问政策以及通过使用网络端口号码安装过滤器。

●互联网访问政策。多个过滤器可以用作互联网访问政策。当你想编辑一个，在下拉菜单中选择政策号码。标签更改反映此政策的设置。如果你想删除此政策，点击**删除**按钮。要看所有政策的汇总，点击**汇总**按钮。汇总列在 7-23 图所示的屏面上以及其名称和设置。返回过滤器标签，点击**关闭**按钮。

●输入政策名称。在此处所示的字段里创建政策。
  创建互联网访问政策：

1．在提供的字段里输入政策名称，选择**互联网访问**作为政策类型。



6-22 图：访问限制

2．点击**编辑表单**按钮，这将打开 6-24 图所示的个人计算机屏的表单。在此屏上，你可输入任何此政策将适用于的个人计算机的 IP 地址或 MAC 地址。你甚至可通过 IP 地址输入个人计算机的范围。点击**申请**按钮保存你的设置，点击**取消**按钮取消任何的改动，点击**关闭**按钮返回至过滤器标签。

3．如果你想否认或允许你列在个人计算机屏上的这些个人计算机的互联网访问，点击选项。

4．你可以通过在阻塞服务旁的下拉菜单中选择一个服务来过滤访问通过互联网已访问的各种服务诸如 FTP 或 Telnet。如果服务没被列出，你可点击**添加服务**按钮打开 6-25 所示的服务屏并把服务添加到表单中。你需要输入服务名称以及服务所用的协议和端口范围。

5．当互联网访问将被过滤时，在日期和时间旁选择正确的设置。

6．最后，点击**保存设置**按钮激活此政策。

创建一个入站交通政策

1． 在提供的字段里输入一个政策名称，选择**入站交通**作为政策类型。
2． 输入你想阻塞的 IP 地址，选择协议：TCP、UDP 或**两个兼顾**，输入**端口**号或选择**任何**，输入你要阻目的 IP 地址。
3． 正确选择**否认**或**允许**。
4． 当入站交通将被过滤时，在日期和时间旁正确选择设置。

最后，点击**保存设置**按钮激活此政策。

当在此标签上改完后，点击**保存设置**按钮保存这些改变或点击**取消改变**按钮取消你的改变。

互联网访问还通过 URL 地址以及以 URL 地址字段方式在网站阻塞中的一个输入地址得到过滤。如果你不知道 URL 地址，过滤可以密码字段方式在网站阻塞中的一个输入一个密码来密码进行。

6-23 图：互联网过滤器汇总

6-24 图：个人计算机表单

6-25 图：阻塞服务

应用程序及对策标签

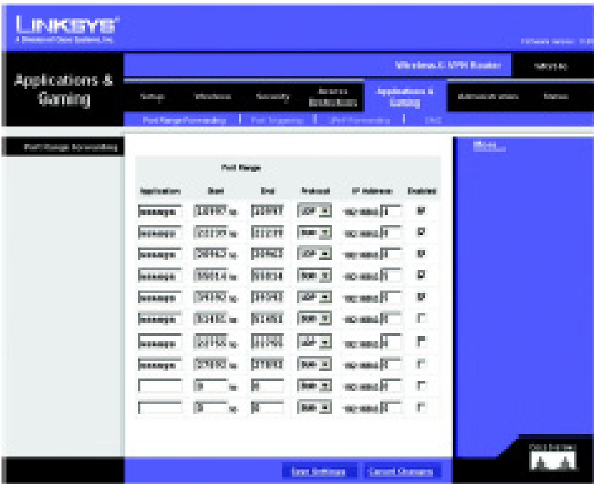
端口范围寄送

在你的个人网络上端口发送屏装有公共服务如：web 服务器、ftp 服务器、e-mail 服务器或其它专用互联网应用程序。（专用互联网应用程序是使用互联网访问诸如视频会议或在线对策性能的任何应用程序。一些互联网应用程序不可以请求任何寄送。）（见 6-26 图）

当用户通过互联网向你的网络发送此类请求时，路由器将把这些请求寄到正确的个人计算机，任何个人计算机的端口被寄送的计算机必须让它的 DHCP 客户功能停止并且必须分配一个新的固定的 IP 地址给它，因为当使用 DHCP 功能时，它的 IP 地址可以改变。

- 申请。输入你想申请的名称。
- 开始和结束。输入你想寄送的端口的开始和结束号码。
- 协议。选择你想用于每个应用程序的协议类型：TCP、UDP 或**两个兼顾**。
- IP 地址。输入 IP 地址，点击**启动**。

当在此标签上改完后，点击**保存设置**按钮保存这些改变或点击**取消改变**按钮取消你的改变。



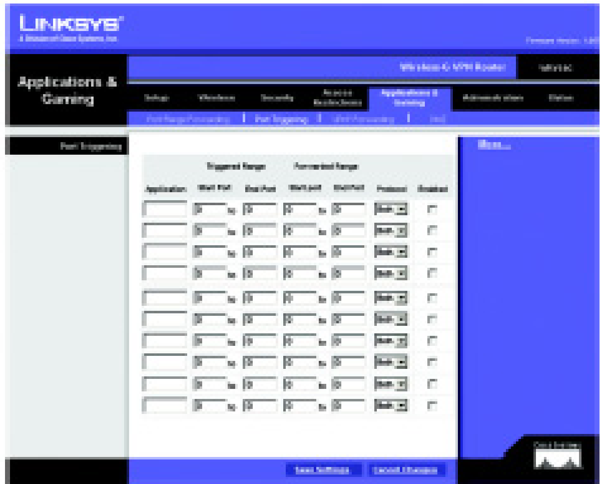
6-26 图：端口范围寄送

端口触发

端口触发用于输出端口不同于进入端口的专用互联网应用程序。使用此性能，路由器将察看专用端口号码的输出数据。（见 6-27 图）路由器将记住发送传送请求数据的计算机的 IP 地址以便当请求数据通过路由器返回时，数据途径 IP 地址和端口路线返回到正确的计算机。

- 申请。输入你想申请的名称。
- 开始和结束端口。输入你想寄送的端口的寄送触发范围号码以及开始和结束触发范围号码。
- 协议。选择你想用于每个应用程序的协议类型：TCP、UDP 或**两个兼顾**。
- IP 地址。输入 IP 地址，点击**启动**。

当在此标签上改完后，点击**保存设置**按钮保存这些改变或点击**取消改变**按钮取消你的改变。



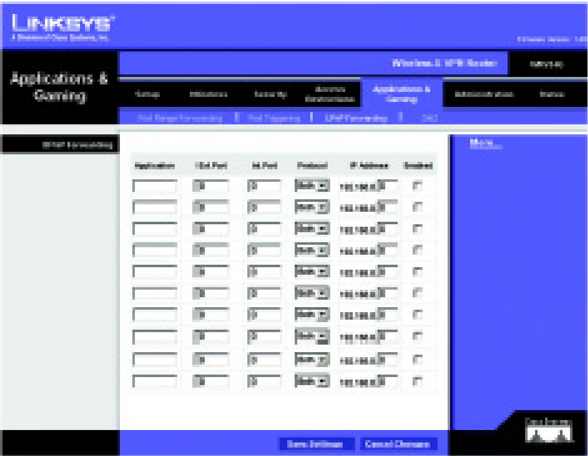
6-27 图：端口触发

UPnP 寄送

UPnP 屏向应用程序的端口服务的自定义提供选项。（见 6-28 图）

在字段里输入应用程序,接着在字段里输入外部和内部端口号码,选择你想用于每个应用程序的协议类型:TCP、UDP 或**两个兼顾**，在字段里输入 IP 地址。针对已选的申请，点击**启动**，启动 UPnP 寄送。

当在此标签上改完后，点击**保存设置**按钮保存这些改变或点击**取消改变**按钮取消你的改变。



6-28 图：UPnP 寄送

DMZ

DMZ 屏（见 6-29 图）允许一个本地用户通过 DMZ 软件接触互联网使用如互联网对策和视频会议专用服务，或用户可通过 DMZ 硬件使用局域网端口 4 作为 DMZ 端口。鉴于端口范围寄送仅能寄送最多 10 个范围端口，DMZ hosting 为一台个人计算机同时寄送所有端口。



6-29 图：DMZ

● DMZ 软件。此性能允许一个本地用户接触互联网使用如互联网对策和视频会议专用服务。使用此性能，选择**启动**。停止 DMZ，选择**停止**。

● DMZ 主 IP 地址。接触一台个人计算机，请输入计算机的 IP 地址。要获得一台计算机的 IP 地址，参照"附录 D：查找你 Ethernet 适配器的 MAC 地址和 IP 地址"。通过在字段里输入一个 0 来使 DMZ 无效。

● DMZ 硬件。此性能允许用户使用局域网端口 4 作为 DMZ 端口。使用此性能，选择**启动**。停止 DMZ，选择**停止**。

● DMZ 硬件地址。在字段里输入计算机的 IP 地址。

● DMZ 硬件网屏蔽。在字段里输入网屏蔽。

● 目的地 IP 地址。在字段里输入目的地的 IP 地址。

● 子网掩码。在字段里输入目的地的子网掩码。

● 默认网关。在字段里输入默认网关。

● 米制。在字段里输入米制。

当在此标签上改完后，点击**保存设置**按钮保存这些改变或点击**取消改变**按钮取消你的改变。

管辖标签

管理

6-30 图显示的管理屏允许你改变路由器访问设置以及配置 SNMP 和 UpnP（通用即插即用）性能。



6-30 图：管理

路由器密码

本地路由器访问。为了确保路由器的安全，当你访问路由器网基实用程序时，要求你提供密码。默认密码是 admin。

- 用户名。输入默认 admin。
- 路由器密码。建议你改变把默认密码改为你选择的一个。
- 重新输入确认。重新输入路由器新密码确认。

路由器访问。此性能允许你通过互联网远程访问路由器。

- 远程管理。此性能允许你通过互联网远程管理路由器。启动远程管理，点击**启动**。
- 管理端口。从下拉菜单上选择你将用于远程访问路由器的端口号码。

SNMP

简单网络管理协议（SNMP）是一个普及的网络监视和管理协议。启动 SNMP，点击**启动**。停止 SNMP，点击**停止**。

- 识别。在联系字段里，输入路由器的联系信息。在装置名称字段里，输入路由器的名称。在位置字段里，说明路由器所在的区域或位置。
- 获得共享。输入允许只读访问路由器 SNMP 信息的密码。
- 设置共享。输入允许只读/写访问路由器 SNMP 信息的密码。
- SNMP 受托主机。你可通过 IP 地址限制访问路由器的 SNMP 信息。在 SNMP 受托主机字段里输入 IP 地址。如果此字段留有空白，那么许可从任何的 IP 地址访问。

- SNMP 陷阱区。输入接收路由器发出的陷阱信息或通知的远程主计算机要求的密码。
- SNMP 陷阱目的地。输入接收陷阱信息的远程主计算机的 IP 地址。

UPnP

UPnP 允许 Windows XP 自动为如对策和视频会议等各种互联网应用程序配置路由器。启动 UpnP，点击**启动**。

- 允许用户作配置改变。当启动时，此性能允许你仍使用 UPnP 性能作手动改变。
- 允许用户停止互联网访问。当启动时，此性能允许你禁止任何和所有互联网连接。

当在此标签上改完后，点击**保存设置**按钮保存这些改变或点击**取消改变**按钮取消你的改变。

记录

6-31 图所示的记录标签为你的互联网连接向你提供所有入出 URLs 或 IP 地址的记录。

邮件警报
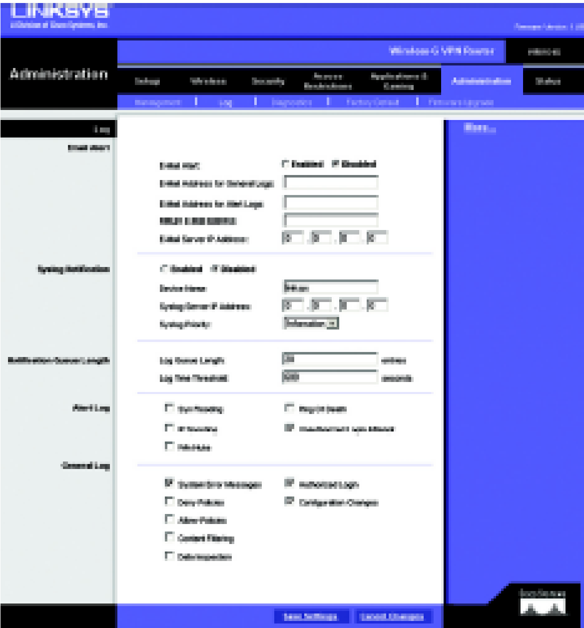
启动电子邮件警报，点击**启动**。

- 一般记录的电子邮件地址。在字段里输入**一般记录的电子邮件地址**。
- 告警登录的电子邮件地址。在字段里输入**告警登录的电子邮件地址**。
- 返回电子邮件地址。输入**返回电子邮件地址**。
- 电子邮件服务器 IP 地址。在字段里输入**电子邮件服务器的 IP 地址**。

系统记录通知

启动系统记录，点击**启动**。

- 装置名称。在字段里输入**装置名称**。



6-31 图：记录

● 系统记录服务器 IP 地址。输入系统记录服务器的 IP 地址。
● 系统记录优先权。从下拉表单上选择**优选权**。

通知序列长度

● 记录序列长度。在字段里输入记录序列里的条目数。
● 记录时间阀。在字段里输入**阀时间**。

告警登录

选择要警报你的袭击类型。选择 Syn Flooding， IP Spoofing， Win Nuke， 死 Ping 或未经授权的登录。

一般记录

选择你想记录的活动类型。选择系统错误信息，否认政策、允许政策、内容过滤、数据检查、授权登录或配置改变。

当在此标签上改完后，点击**保存设置**按钮保存这些改变或点击**取消改变**按钮取消你的改变。

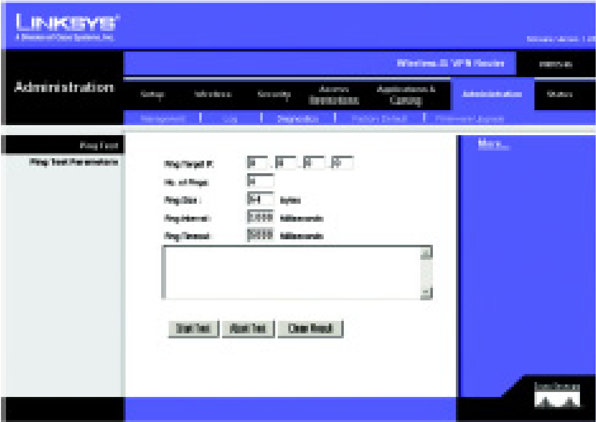
诊断

Ping 测试 （见 6-22 图）

Ping 测试参数

Ping 目标 IP。在字段里输入你要 Ping 的 IP 地址。
无 Ping。输入你要 Ping 的时间数。
Ping 尺寸。输入 Ping 包的尺寸。
Ping 间隔。用秒输入 Ping 间隔。
Ping 超时。用秒输入时间。

点击**启动测试**按钮启动 Ping 测试。点击**中止测试**按钮停止测试。点击**清除结果**按钮清除结果。测试结果将在窗口里显示。



6-32 图：Ping 测试

工厂默认（见 6-32 图）

如果你用完了其它所有选项并想把路由器恢复至工厂默认设置，丢掉所有你的设置，点击**是**。

当在此标签上改完后，点击**保存设置**按钮保存这些改变或点击**取消改变**按钮取消你的改变。



6-33 图：工厂默认

固件升级（见 6-34 图）

升级路由器的固件：

1．点击**浏览**按钮查找你从 Linksys 网站下载并解压缩的固件升级文档。

2．双击你下载并解压缩的固件文档。点击**升级**按钮，按上面的说明。



6-34 图：固件升级

状态

路由器

此屏显示你的路由器和它的 WAN（互联网）连接的信息。（见 6-35 图）

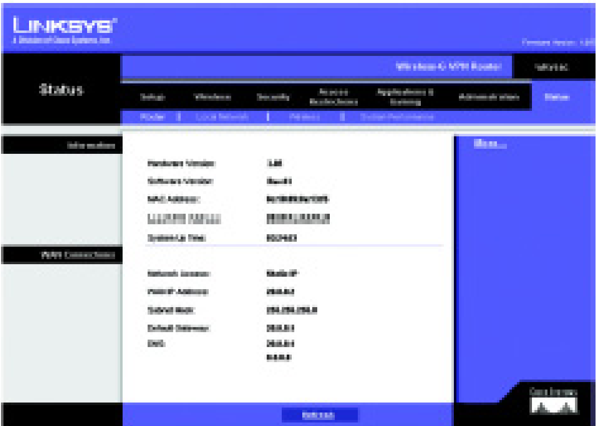
信息

所显示的信息是硬件版本、软件版本、MAC 地址、本地 MAC 地址和系统有效时间。

WAN 连接

所显示的 WAN 连接是网张访问、WAN IP 地址、子网掩码、默认网关和 DNS。

如果你要刷新你的屏面，点击**刷新**按钮。



6-35 图：路由器

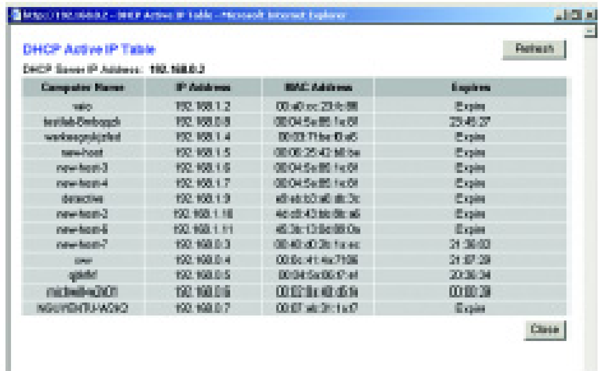
局域网

所显示的局域网络信息是 IP 地址、子网掩码、DHCP 服务器和 DHCP 客户租赁信息。浏览 DHCP 客户标签，点击 DHCP 客户按钮。见 6-36 图。

6-37 图所示的 DHCP 活动 IP 标签显示计算机名、IP 地址、MAC 地址和终止时间。点击关闭按钮返至局域网络屏。



6-36 图：局域网络

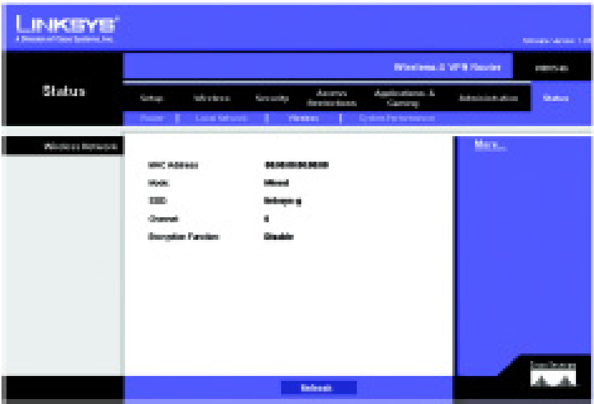


6-37 图：DHCP 活动 IP 标签

无线

所显示的无线网络信息是 MAC 地址、模式、SSID、通道和加密功能。（见 6-38 图）

如果你要刷新你的屏面，点击**刷新**按钮。



6-38 图：Wireless

系统性能

所显示的系统性能信息是无线、互联网和/或 IP 地址、MAC 地址、连接状态、已收的包、已发的包、已收的字节、已发的字节、已收的错误包和已收的损失包的局域网信息。（见 6-39 图）

如果你要刷新你的屏面，点击**刷新**。



6-39 图：系统信息

附录 A：疑难问题解答

该附录包含两大部分：“一般问题解答”和“常见问题解答”
提供一些安装和使用路由器过程中可能会出现的问题及解决方法。
阅读以下说明，它能帮助你解决遇到的难题。如果你不能在这里找到解决方法，你可以登陆我们的网站：
www.linksys.com

一般问题的解决：

1 我需要在计算机上设置一个固定 IP 地址。
你可以按以下操作步骤获得一个固定 IP 地址：
WINDOWS 98/ME 操作系统：
1 点开始菜单，点设置，进入控制面板，双击网络。
2 在网络组件中选择 TCP/IP，根据你的以太网适配器选。如果你仅安装了以太网适配器，你只看见 TCP/IP 线，和以太网适配器没有关联。选中 TCP/IP，点击属性键。
3 在 TCP/IP 属性窗口里，选择 IP 地址标签，选择指定一个 IP 地址，进入了一个独一无二的在网络上与路由器相连的 IP 地址，确认该 IP 地址唯一性。
4 点击 GATEWAY（网关）标签，键入 192.168.1.1，这是路由器的默认 IP 地址。点击添加确认输入。
5 点击 DNS 标签，确认 DNS 项被选中，输入主机名，组)。输入由你的网络服务商提供的 DNS。如果你的网络服务商没有提供 DNS IP 地址，则联系他们，得到相关信息或登陆他们的网站。
6 点击 TCP/IP 属性窗口的 OK 键，点关闭或网络窗口的确定键。
7 重新启动计算机。

WINDOWS 2000 操作系统：
1 点击开始菜单，进入设置，点控制面板。双击网络和拨号上网。
2 右击本地连接，选择属性
3 选中“TCP/IP 协议”，点属性键，选使用以下 IP 地址选项。
4 选择网上路由的唯一性 IP 地址。
5 输入子网掩码，255.255.255.0

6 输入默认网关：192.168.1.1（路由器默认 IP 地址）
7 在窗口底部选择使用以下 DNS 服务器地址，并且输入首选 DNS 服务器和可替代 DNS 服务器（由你的网络服务供应商提供）。联系你的网络服务供应商或登陆他们的望站获得相关信息。
8 在 TCP/IP 协议属性窗口点确定，再在本地连接窗口点确定。
9 重新启动计算机

WINDOWS XP 操作系统：
以下操作假设你运行的是 WINDOWS XP 操作系统界面。如果你用的是老式界面，请根据 WINDOWS 2000 操作系统来。
1 点开始菜单，进入控制面板
2 点网络和拨号上网，进入网络连接标识
3 右击本地连接，选择属性
4 在连接运用以下项目框里，选 TCP/IP 网络协议，点属性键
5 输入唯一性的 IP 地址
6 输入子网掩码 255.255.255.0
7 输入默认网关：192.168.1.1（路由器默认 IP 地址）
8 在窗口底部，选择 DNS 服务器地址，输入首选服务器和可替代服务器（由你的网络服务供应商提供）。和你的网络供应商联系或登陆他们的网站获得相关信息。
9 点 TCP/IP 属性窗口的确定键。点本地连接的确定键。

2 我想测试我的互联网连接
A 核对你 TCP/IP 设置
WINDOWS 98，ME，2000，XP 操作系统：
- 详细参阅：第四章：计算机参数设置确认，自动获得 IP 地址功能的设置。

WINDOWS NT 4.0 操作系统：
- 点开始菜单，设置，进入控制面板，双击网络
- 点协议标签，双击 TCP/IP 协议
- 当窗口出现，确认选择了正确的网络适配器并且确认从 DHCP 服务器上获得一个 IP 地址设置。
- 点 TCP/IP 协议属性窗口的确定键，再点网络窗口上的关闭键。
- 重新启动计算机

B 打开一个命令提示符。
WINDOWS 98/ME 操作系统:
●点开始菜单，运行，用命令打开字段，类型。按回车键或按确定。
WINDOWS NT，2000，和 XP 操作系统:
●点开始菜单，运行，用命令打开字段，类型。按输入键或按确定。在命令提示符，输入 PING 192.168.1.1，按回车。
●如果你得到回应，计算机正在与路由器交互。
●如果你没有得到回应，请检查光缆网络，确认设置为自动获得一个 IP 地址，再次在命令提示符下，键入 PING 192.168.1.1 命令，回车。
C 在命令提示符下，键入 PING INTERNT 地址或 WAN IP 地址，按回车
互联网或 WAN IP 地址能在路由网络运用的状态显示屏被找到。举个例子你的互联网地址或 WAN 地址是 1.2.3.4，你输入 PING 1.2.3.4，回车。
●如果有回应，计算机与路由正确连接。
●如果没回应，从另一台计算机输入 PING 命令，以确认你自己计算机没问题。
D 在命令提示符下，键入 PING www.yahoo.com，按回车
●如果有回应，你的计算机与互联网连接好。如果不能打开网页，则从另一台计算机上执行该命令以确认你的计算机没问题。
●如果没有回应，也许是连接的问题，再从另一台计算机上运行 PING 命令，确认你自己的计算机没问题。

3 我没有在互联网上得到 IP 地址。
●参阅“难题 2：我想测试我的互联网连接”确认你是否连接在网上。
1 如果你要你的网络服务供应商提供注册你的以太网适配器的 MAC 地址，请参阅“附录 D：找出 MAC 地址和 IP 地址”，如果您需要客隆你连接到路由上的以太网适配器 MAC 地址，见系统部分“第六章：路由器的网络利用”。
2 确认你在使用互联网连接设置。联系你的网络服务供应商看你的网络连接类型是否是 DHCP，固定地址是否正确，或 PPPOE（一般被用在 DSL 用户上）。请参阅设置信息部分“第六章：路由器网络的运用”关于互联网连接设置部分。
3 确认你的光缆网络正确连接，确认你的 LINK/ACT 网络指示灯是否正常。
4 确认光纤是否与路由上的 INTERNENT 端口正确连接。确认状态页面上的 IP 地址是否有效。
5 关闭计算机，路由，调制解调器。等待 30 秒，然后重新打开各网络设备。确认你的 IP 地址是否有效。

4 我不能进入路由网络使用的安装设置页面。

●查阅“难题 2：我想测试我的互联网连接”，确认你的计算机与路由连接正确。

1 查阅“附录 D：找出你以太网适配器的 MAC 地址和 IP 地址”，确认你的计算机 IP 地址，子网掩码，网关，还有 DNS 状态。

2 在你的计算机上设置 IP 固定地址；参阅“难题 1：我需要设置一个固定 IP 地址”

3 参阅“难题 10：我需要删除代理服务器设置或拨号上网窗口（PPPOE 用户）。”

5 我不能通过路由建立 VPN 虚拟隐私网络。

进入路由网络界面：HTTP：//192.168.1.1 或输入路由的 IP 地址，进入安全标签，确认你的 IP 安全策略或 PPTP 通过处于激活状态。

●VPN IP 安全策略为协议 50 比较合适。至少有一个 IP 安全策略运用在路由上；但是，多个 IP 安全策略可以同步使用，这都依赖你的 VPN 的要求。

●VPN 用的 IP 安全策略还有 AH（协议 51）与路由不兼容。AH 的局限性在于有时他与 NAT 标准不兼容。

●改变路由的 IP 地址到另外的子网，以避免 VPN IP 地址与你的本地 IP 地址冲突。举个例子，如果你的 VPN 服务器和 IP 地址是 192.168.1.X（X 从 1 到 254），你的局域网 IP 地址是 192.168.1.X（X 与 VPN IP 地址数字一样），路由就找不到正确的位置信息。如果你改变路由的 IP 地址为 192.168.2.1，问题就解决了。

●通过网络安装设置界面来改变路由 IP 地址，如果你在网络上给你的计算机或网络设备固定 IP 地址，你需要以 192.168.2.Y 格式去改（Y 从 1-254）。注意每个 IP 地址必须唯一。

●你的 VPN 也许要端口 500/UDP 速度的数据包传到计算机上，这台计算机与 IP 安全服务器连接。参阅“难题 7：我需要建立网上游戏主机或用其他网络应用程序”

●登陆 www.linksys.com 获取更多信息。

6 我要安装设置一个在路由后的服务器，使它公用。

为了使用服务器象网络，FTP，或邮件服务器，你必须知道各自的端口号。举个离子，网络服务器用的端口号是 80（HTTP）；FTP 用的是 21；SMTP 是 25，POP3 邮件服务器是 110。你能在服务器安装文献中找到详细信息。

●根据以下步骤通过路由网络运用来建立端口。我们将要设置网络，FTP，邮件服务器。

1 进入路由网络运用窗口，输入 HTTP：//192.168.1.1 或路由 IP 地址。进入应用程序和游戏，端口标签。

2 输入常规应用你想要的名称。
3 输入你想用的外部端口范围。举个例子，输入 80-80。
4 确认你使用的通讯协议，TCP 和/或 UDP
5 输入你想要的端口服务器上的计算机或网络的 IP 地址。例如，如果你的网络服务器 IP 地址是 192.168.1.100，你在字段里输入 100。查阅“附录 D:找出你的以太网适配器的 MAC 地址和 IP 地址”中获得 IP 地址部分。
6 确认你用端口服务被激活。考虑以下例子:

常规运用	外部端口	TCP	UDP	IP 地址	激活
网络服务器	80-80	X	X	192.168.1.100	X
FTP 服务器	21-21	X		192.168.1.101	X
SMTP 邮件出	25-25	X	X	192.168.1.102	X
POP3 进邮件	110-110	X	X	192.168.1.102	X

当你完成这些设置，点保存设置。

7 我要安装在线游戏主机或使用其他互联网应用程序

如果你要玩在线游戏或用互联网应用程序，大多数没有 DMZ 主机端口。当你想主持在线游戏或用网上应用程序，就有这样的情况。这就要求你设定路由把进来的数据包传到指定的计算机上。这也同样用于互联网应用程序。最好的方法是进入服务端口采集信息，进入你想到的网站得到信息。按以下步骤安装网上游戏或使用互联网应用程序:
1 进入路由网络界面，HTTP: //192.168.1.1 或输入路由 IP 地址。进入应用程序和游戏，点前端口标签
2 输入常规应用程序名
3 输入外部端口范围，例如 UT，输入 7777-27900
4 核对通讯协议，是 TCP 和/或 UDP
5 输入服务器端口要到的计算机或网络设备的 IP 地址。例如，IP 地址是 192.168.1.100，你在空格处输入 100。核对“附录 D: 找出网络 MAC 地址和 IP 地址”中关于获取 IP 地址部分。
6 查看端口服务器的激活选项。举例如下:

常规运用程序	外部端口	TCP	UDP	IP 地址	激活 ENABLE
UT	7777-27900	X	X	192.168.1.100	X
半衰期	27015-27015	X	X	192.168.1.105	X
计算机随放	5631-5631		X	192.168.1.102	X
VPN IP 安全策略	500-500		X	192.168.1.100	X

当你完成设置，点保存设置键。

8 在线游戏，服务器，应用程序不工作。

如果在线游戏，服务器，应用程序不工作，考虑把一台计算机暴露到用 DMZ 的互联网上，当一个应用程序需要太多的端口或当要用的端口服务不确定时，必须要有 DMZ 选项。如果你想成功使用 DMZ，你必须确定取消了前面所有选项。因为前置选项比 DMZ 有优先级。（换句话说，数据进入路由首先被前设置检查，如果没有前端口确认，则路由会把数据传给 DMZ 主机处理）

●按以下步骤设置 DMZ 集合：

1 进入路由窗口，HTTP：//192.168.1.1，或输入路由 IP 地址。进入应用程序和游戏——DMZ 标签

2 禁用前设置，保留上面信息，以防有用。

●完成后，点保存设置键。

9 忘记密码或当保存设置到路由时总是出现密码提示符

●按住复位键 10 秒重新设置默认设置，然后松开。如果还有密码提示符，则按以下步骤操作：

1 进入路由器界面，HTTP：//192.168.1.1 或输入路由的 IP 地址。进入默认口令管理，点管理，口令管理标签。

2 输入不同的路由口令，再输入一次口令。

3 点保存设置键。

10 我是 PPPOE 用户，我要取消代理设置或拨号连接。

如果你有代理设置，你要在你的计算机上取消此设置。因为你的路由是互联网的网关，计算机不需要任何代理设置进入网络。请按以下指导确认你没有任何代理设置，浏览器直接连接在局域网上。

● MICROSOFT5.0 互联网浏览器或更高版本：

1 点开始菜单，设置，进入控制面板，双击互联网选项

2 点连接标签

3 点局域网设置，删除所有内容。

4 点确定，回到前页。

5 点永不拨号连接选项。这就为 PPPOE 用户把拨号上网删除了。

● 网景 4.7 浏览器或更高版本：

1 启动网景浏览器，点编辑，首选项，高级，代理设置。

2 确认直接连接到互联网上。

3 关闭所有窗口，完成。

11 启动结束，我要设置路由的出厂设置

按住复位键十秒，然后放开。这会把口令，前设置，其他设置恢复到路由的出厂设置。换句话说，路由恢复出厂的原始设置。

12 我要进行功能升级。

为了获得最新的功能，对路由进行升级，你要到 LINKSYS 网站上，从 www.linksys.com 下载最新的版本。

● 按以下步骤操作：

1 登陆 HTTP：//www.linksys.com 下载最新组件。

2 为了升级，按以下操作步骤，见“第六章：路由网络运用功能”

13 固件升级失败，电源 LED 指示灯不断闪动。

由于诸多原因，升级可能失败，按以下步骤升级固件，使电源指示灯停止闪动。

● 如果固件升级失败，用 TFTP 程序（可下载）。打开同固件下载的 PDF 文件和 TFTP 程序，按 PDF 文件提示步骤操作。

● 在计算机上设置固定 IP 地址，查阅“难题 1：我要设置一个固定 IP 地址” 用以下 IP 地址设置：

IP 地址：192.168.1.50

子网掩码：255.255.255.0

网关：192.168.1.1

● 用 TFTP 程序运行升级，或通过路由网络运用中的管理标签升级。

14 我的DSL服务的PPPOE总是断线。

PPPOE连接不是专线或一直在线的连接。DSL ISP能在一段静止后，断线，就好象拨号上网一样。

●有一个设置“永远激活”连接。这也不总是有效，有时你要建立时段连接。

1 连接路由，到网络浏览器，输入HTTP：//192.168.1.1或路由IP地址。

2 输入□令。（默认□令是ADMIN）

3 在设置屏幕上，选永远激活，设置20秒再拨号。

4 点保存设置。

5 点状态标签，点连接键。

6 你可以看到连接登陆的状态。按F5刷新屏幕，直到你看到连接上了为止。

●点保存设置继续。

●如果又吊线，按步骤1-6重建连接。

15 我不能使用我的E-MAIL，网络，或VPN，我连不上互联网。

也许要调整最大传输单元MTU，默认设置是1500。对大多数DSL用户，强烈推荐MTU1492

●如果你有困难，按以下步骤操作：

1 为连接路由，进入网络浏览器，输入HTTP：//192.168.1.1或输入路由IP地址。

2 输入□令

3 找到MTU选项，选手动，在大小字段里，输入1492

4 点保存设置，继续

●如上网还有困难，改变大小。尝试以下值直到你的问题解决：

1462

1400

1362

1300

16 电源LED指示灯不断闪动

当电源一打开，LED灯闪动，在这期间，系统执行引导程序，并且检查操作。完成检查后，LED应停止闪动，表明系统工作正常。如果灯闪动，说明设备工作异常。你可以使用固定IP地址扫描固件，然后升级固件。使用以下设置，IP地址：192.168.1.50，子网掩码：255.255.255.0

17 当我输入 URL 或 IP 地址， 我得到超时或要我重试。

●检查其他计算机是否有同样故障。如果他们也这样，确认工作站的 IP 设置正确（IP 地址，子网掩码，默认网关，DNS）。重新启动计算机。

●如果计算机正确设置，但还不能连接，检查路由。确认连接正确，电源开着。进入路由，检查设置。（如果连不上，检查局域网络和电源连接）

●如果路由配置正确，检查互联网连接（DSL/调制解调器等），看他们是否都工作正常。你可以去除路由，用直接连接试一试。

●手动设置 TCP/IP 协议设置，用网络服务供应商提供的 DNS 地址来设置。

●确认你的浏览器连接正确，没有拨号。对于互联网浏览器，点工具，互联网选项，进入连接，确认网络浏览器的设置永不拨号连接。对于网景浏览器，点编辑，首选项，高级，代理设置。确认是直接连接到 INTERNENT。

常见问题解答:

路由支持 IP 地址最大值:

253

路由支持 IP 安全策略通过选项吗？

是的，该路由器有此功能

路由安装在网络的哪个位置？

在一个典型的网络环境中，路由器被安在光纤或 DSL 调制解调器和局域网络之间。把路由器插进光纤或 DSL 猫的以太网端口上。

该路由器支持 IPX 或 APPLETALK 吗？

不。TCP/IP 是互联网的协议标准，成为全球通讯标准。IPX，是网景通讯协议，仅用在从一个网络节点到另一点；APPLETALK 是苹果网和 MACINTOSHI 网络的通讯协议，用在局域网和局域网（LAN）之间，他们的协议不能连接互联网到局域网上。

该路由的互联网连接支持 100Mbps 以太网吗？

该路由器硬件设计支持互联网端口上 100Mbps 的以太网;但是,互联网连接速度变化依赖宽带速度的变化。该路由器也支持在路由局域网络这一边的自动感应快速以太网 10/100 交换器。

NAT 是什么，它有什么功能？

NAT 把在隐私局域网络上的多个 IP 地址转到一个公用地址上，然后送到互联网上。另外，NAT 允许路由使用便宜的互联网帐户，例如 DSL 或调制解调器，当网络服务供应商提供 TCP/IP 地址。用户在网络服务供应商提供 IP 地址后可以有多个个人隐私地址。

除了 WIDNOWS 95/98/MILLENNIUM/2000/XP 以外，还支持其他那些操作系统？

是。但现在 LINKSYS 公司没有提供技术设置，配置文件或非 WINDOWS 操作体统的问题解决。

该路由器支持 ICQ 发送的文件吗？

是，用以下设置：点 ICQ 菜单，点首选项，连接，确认是否在防火墙或使用代理服务器。在防火墙设置中，设置 80 秒。互联网用户能在路由器后发送文件。

我建立虚拟的服务器，但是局域网上其他不能加入。我该怎么做？

如果你运行一个虚拟的比赛服务器，你要为本地计算机用户建立一个固定 IP 地址，IP 地址服务器上前端口是：7777，7778，7779，7780，7781 和 27900。可选范围是 7777-27900。如果你想用 UT 服务管理器，前到另一端口。（端口 8080 好用，但用于远程管理。你不得不禁止它） 在网络服务器部分，设置监听端口为 8080（与以上端口对应）并且确认服务器名到网络供应商提供的路由 IP 地址。

局域网上的多个游戏者，能否同时使用一个公用 IP 地址？

这依赖网络游戏或他们在用的游戏服务器。例如，虚拟比赛服务器支持多人用一个公用 IP 地址登陆。

我怎样得到 HALF-LIFE：团队堡垒能用这个路由吗？

HL 的默认客户端口是 27005。局域网上的计算机需要有“+客户端口 2700X”加上 HL 快捷命令线；X 可以是 6，7，8 等以上数字。这允许多个游戏者连接到同一服务器上。一个问题：版本 1.0.1.6 不允许多人同步连接。即使在同一个局域网上的多个用户。就主机游戏而言，HL 服务器没有必要在 DMZ 上。仅把前端口 27015 连到计算机服务器的本地 IP 地址上。

我怎样结束错误的 FTP 下载？

当你用你的 FTP 客户端下载过文件，你一定经历过坏文件，重使用另一个 FTP 程序。

网页挂起；下载失败，在屏幕上显示乱码。你怎么办？

使你的以太网适配器达到 10MBPS 的速度或半双向模式，关闭自动连接暂时功能。（请查看控制面板上的以太网适配器高级属性设置。确认浏览器的禁止使用代理服务器设置。在 www.linksys.com 查更多的信息。

装载失败怎么处理？

按住复位键直到 LED 电源指示灯熄灭，再打开，重新设置。复位调制解调器电源。找到安装最新的固件，上网下载：www.linksys.com

我怎样知道有新的固件升级？

所有的固件升级在 www.linksys.com 上都可以找到，免费。要升级你的路由器固件，用系统标签。如果路由网络连接正常，没有必要下载更新的版本，如果那个版本没有什么你想用的新功能。下载一个更新的路由器版本不会提高你的互联网连接速度与质量，也许会破坏你现在连接的稳定性。

路由器在 MACINTOSH 操作环境下有用吗？

是的。但是路由器页面通过互联网浏览器 4.0 或网景浏览器 4.0 或 MACINTOSH 更高版本接入。

我不能进入路由器的网络配置页面，我该怎么处理？

你删除你的互联网浏览器的代理设置。或删除拨号设置。检查你的浏览器文献，确认你的浏览器是直接连接到网络，拨号无效。对于网络浏览器，点工具，网络选项，连接。确认设置为永不拨号连接。对于网景浏览器，点编辑，首选项，点高级选项，代理服务器。确认是直接连接设置。

什么是 DMZ 主体模式？

DMZ 允许一个 IP 地址暴露到互联网上。一些应用程序需要多个 TCP/IP 端口开放，如果你想用 DMZ 主机功能，建议设置一个固定 IP 地址。为了得到这个局域网 IP 地址，查阅“附录 D：找出 MAC 地址和你的以太网 IP 地址”

如果使用了 DMZ 不设防功能，被暴露的用户和路由共享 IP 地址吗？
不。

路由器通过的是 PPTP 数据包还是使用分时发送数据包？
路由器允许 PPTP 数据包通过。

路由器平台可以兼容吗？
任何支持以太网和 TCP/IP 通讯协议的平台都与该路由器兼容。

前设置上有多少同步端口？
理论上讲，可以同时 520 个分时用户，但实际中只在 100 以内端口。

这种路由器先进功能在哪？
包括无线设置，过滤功能，前端口，寻址功能，还有 DDNS 功能。

路由器允许的 VPN 分时最大是多少？
因素很多。至少一个安全策略分式要穿过路由器；但是，同步 IP 安全分时的数目也依赖你的 VPN 的数目。

我怎样才能知道我是否有固定或 DHCP IP 地址？
向你的网络供应商咨询获得此信息。

这种路由器可以作为我的 DHCP 服务器使用吗？
是的。路由器有 DHCP 服务器内置软件。

我能运行远程计算机上的应用程序，通过无线连接？
这就要看该应用程序是否为网络设计。查看应用程序文献确认它是否支持网络操作。

什么是 IEEE802.11G 标准？
它是无线网络的 IEEE 标准。它使从不同供应商来的网络硬件可以兼容交互，他们都运用 802.11G 标准。
802.11G 标准代表最大传输速度为 54MBPS，操作频率是 2.4GHZ

IEEE802.11B 有那些功能？

- CSMA/CA 外加通知协议功能
- 多信道漫游功能
- 自动比率选择
- RTS/CTS 功能
- 分块功能
- 电源管理

什么是 AD-HOC 模式？

当一个无线网络被设置到 AD-HOC 模式，无线网络里的计算机可以直接交互。AD-HOC 无线网络不能与有线网络交互。

什么是基础模式？

无线网络设置为基础模式，无线网络可以通过一个无线接入点与有线网络交互。

什么是漫游？

漫游是指并不局限于某个接入点，而是手提电脑用户自由穿梭某个区域。在使用漫游功能前，工作站必须确认信道号码与专有接入点覆盖区域号码相同。

为了获得真正的自由连接，无线局域网络必须配有很多不同功能。例如，每个网络节点和接入点必须总能提供接受信息。每个节点必须保持与无线网络连接即使没有在传输数据。同时获得这些功能，同步要求一个动态的 RF 网络技术使接入点与网络节点连接。在这样的一个系统里，用户节点试图找到最佳点接入系统。首先，它估量这样一些因素，信号强弱，信号质量，目前装载信息，每个接入点与有线工作站的距离。基于这样的信息，网络节点下一步选择正确的接入点，然后注册地址。终端和主机就可以通过工作站信号发射台来传输信息。

当用户继续移动，计算机的 RF 发射器会决定继续用原来的点接入还是重新确认点接入。当一个节点不再从原来接入点得到信息，它就会寻找新的接入点。找到新的接入点，重新注册，然后继续通讯。

什么是 ISM 波段？
FCC 和他们的美国外的对手在工业，科学，医疗规定的波段宽度。2.4GHZ 尤其常用。在全球用户手中，ISM 提供了真正的革命性的使用高速无线网络的机会。

什么是展开光谱？
展开光谱技术是从军事通讯发展来的，安全，可靠，是军事中非常重要的集团通讯手段。它无须考虑带宽，生成了可靠，一致，安全的网络通信。换句话说，通讯中带宽的选择余地更大了，但实际上 TRADE-OFF 生成了更响也容易接收到的信号，如果接收人知道参数设置，就能收到这样展开光谱信号。如果调的频率不对，一个展开光谱信号就好象噪音。有两种主要的展开光谱：直接序列光谱 DSSS 和多变跳跃展开光谱 FHSS。

什么是 DSSS？什么是 FHSS？有什么不同？
FHSS 利用窄带载体，按固定模式变换频率，双方发射器和双方接受者都知道的模式变化。信号同步，网络效果保持单一逻辑渠道。对于非目的接受器，则是短的噪音。DSSS 是一种完全传输模式。碎片越长，被破译可能就越大。即使传输过程中，碎片码部分丢失了毁坏了，嵌套在广播里的统计技术也可以恢复信息内容。到非目的接收器，DSSS 宽带噪音，或被窄带接收器忽略。

信息在传输过程中可能被截取了吗？
WLAN 有两头安全保护。在硬件上，使用 DSSS 技术，它有安全保密功能。在软件上，WLAN 提供安全加密和接入控制功能。

什么是 WEP？
WEP 是有线等量隐私，数据隐私机械建立在 64 位或 128 位运算法则上，见 IEEE802.11 标准。

什么是 MAC 地址
MAC 地址是制造商给以太网设备的唯一性的符号，例如一个网络适配器，这个符号让网络以硬件水准去识别它。为了所有实际用途，这个号码通常不变。不象 IP 地址，每次登陆到计算机就改变。一个网络设备的 MAC 地址始终不变，让网络好识别。

怎样重设置路由器？

按后面板上的复位键 10 秒。恢复路由的默认设置。

怎样解决信号丢失的问题？

我们没法知道你的无线网络的测试范围。在路由器和一台无线计算机间任何障碍物都会引起信号损失。铅玻璃，金属，混凝土地面，水，墙都会吸收信号减弱信号。先把路由器和你的无线计算机放在同一个屋子里，然后移动计算机，看可以放的最大范围是多少。

你也可以使用不同频道，这可以消除某些特定的频率干扰。

信号很强，但看不到我的网络。

WEP 可能在路由上激活，但没连在无线适配器上。确认同一 WEP 密码和水平（64 或 128 位）用在所有的无线网络节点上。

路由器提供了多少频道或频率？

11 个频道，1-11

如果你还有其他问题，请登陆 www.linksys.com/cn

附录 B：无线安全

概述：

当数据一一以文件，邮件，或消息的形式在无线网络上传输的时候，它是易受攻击的。无线网络危险因为它以无线电波形式传播信息。这样的信号能被截取，从你的无线网络出来的信号也能被截取。无线网络的危险是什么呢？

危险是什么？

计算机网络黑客已不是什么新鲜名词了。随着无线网络的出现，黑客用各种手段盗取你的信息。方法很多，简单复杂都有。作为无线网络用户，你应该知道他们的方法。

当一个无线传输被发射出去，信号从你的计算机或路由器被送出去，但并不直接到达目的地。接收计算机或路由能听到信号因为在发射半径内。就好象无绳电话或移动电话或任何的无线电设备，只要在信号半径内，用同一频道就能接受那些信息。

无线网络很容易被发现。为了加入一个无线网络，黑客首先让你的无线计算机听到 BEACON 消息。这就是典型的无线网络数据包传输的方式，然后再和网络节点连接。这些消息里含有很多未被加密的网络信息，例如网络 SSID 信息，网络计算机，路由 IP 地址。包括网络的名字，有了信号半径内的这些信息，黑客很容易就进入网络。

这样的结果就使很多大城市或社区，成了“星际争霸”。这是形容黑客自由出入宽带网络的术语，他们任意接入无线网络。他们很容易造成网络城市各环节的混乱。

即使保留你的网络设置，例如 SSID 和频道，这也挡不住黑客获取你的登陆信息。这就是为什么无线网络专家强烈推荐 WEP。WEP 加密你的无线信号，使你仅在你的无线网络上被确认。

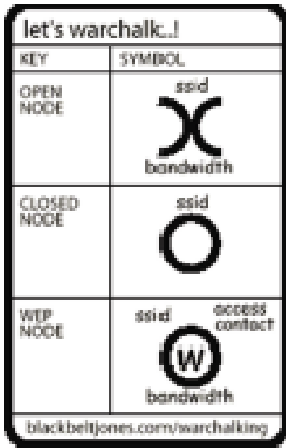


图 B-1：warchalking

但即使 WEP 也有它的弱点。WEP 的加密法则，也很“简单”，也很薄弱，因为对一些专业黑客破译密码不是什么难事。

通常有 5 种常见的黑客攻击你的网络，偷取你数据的方式。如下：

1 被动攻击
2 阻断信道攻击
3 主动攻击
4 统计分析攻击
5 截取攻击

被动攻击

很难觉察被动攻击，因为他不破坏你的网络。他只是监听你的网络，看你的网络信息。很容易可以找到这样的网络软件使他人能监控你的信息。信息包括你的 MAC 地址，IP 地址，用户名，口令，及时交互信息，邮件，帐户信息，任何无线传输的信息很容易就被外人以文本方式打开。很显然，任何传输的信息很容易在网上受到攻击。黑客所要的就是数据包截取器，在网上就有这样的软件，还有其他自由出入软件和共享软件，黑客常使用去获得你的 WEP 密码，其他网络安全信息以穿过防火墙等安全措施。

阻断信道攻击

阻断信道攻击，就是当一个超强信号被直接送到你的无线网络的时候，切断你的无线网络。这一类型的攻击是无目的性，技术简单。尤其在 2.4GHZ 频率，它让电话，小的显示器，微波炉有很大的干扰，阻塞你的无线通道。解决这样攻击的一种途径就是频率改为 5GHZ，专用在信息传输上。

主动攻击:

黑客主动攻击有三个目的: 1 偷数据 2 使用你的网络 3 修改你的网络设置以便下次容易登陆。

在主动攻击里，黑客得到了你的所有网络设置信息。一旦你上无线网络，黑客进入你的网络资源，在你网络上盗取数据。另外，如果无线网络路由器连到交换器上，黑客也可以得到有线网络的数据。

另外，垃圾程序会连接你的互联网，让你的 ISP 邮件服务器，不停发送垃圾邮件。

最后，黑客很容易进入你的网络，穿过你的防火墙，MAC 地址过滤器，穿过加密。他们甚至能偷你的口令和用户名，下次随时登陆你的网络。

统计分析攻击:

建立数据库或表格，这是一种获取网络设置的方法，大多数分析商务网络。时间一常，通过统计数据分析，然后破译所有无线传输信息。这样的攻击更有效，例如商务活动中。

截取攻击

黑客不用进入你的用户网络——他作为网络自身的路由器，就好象站在中间的一个人。黑客要用你的网络设置来配置一个路由器，发出强烈的信号。用这种方法，迷惑你的计算机，让他们把信息送到黑客的路由器上。

带有 TRADE-OFF 功能的灵活无线网络使黑客的这种攻击成为可能-。用无线网络，WEP 加密，对高级黑客开放，你怎么能保护你的数据？以下部分告诉如何保护自己的数据:

网络安全最大化

安全专家会告诉你同样一件事: 没有万无一失的事。没有技术本身是安全的。有时侯，塞翁失马。以下例子里，网络安全措施的实施管理让无线安全最大化。

没有预防措施保证网络安全但可以让黑客很难进来。经常黑客寻找一个容易的目标。使你的防护好些，黑客自然兴趣不大，他们也难进来。

怎样做呢？在讨论 WEP 前，让我们看一些经常容易被忽视的安全措施：

1 网络内容

现在你知道无线网络有很大的危险性。所以不要在无线网络上接入系统或设置主系统，不要把很多东西放在网上。

2 网络布局

当你第一次布局你的网络，仔细想好你的无线计算机位于哪里，尽量在网络半径范围内。记住接入点在辐射范围内，接入点放在物理网络区域边缘减少了网络的运行，很容易受到传输时黑客攻击。

截取攻击通常会发出邀请，这样黑客必须靠近你的网络。所以监视你的网络和属性很重要。另外，你如果怀疑有黑客侵入，要求所有功能登陆认证，你可以确认是否有未授权的登陆。

3 网络设备

记住你使用的每一个无线网络设备的设置，存在固件里。如果到了黑客手里，那就很糟糕了。所以一定看好你的网络设置

4 管理员口令

只有你的网络管理员可以改变网络设置。如果黑客有了密码，他也能该设置。所以一定不能让黑客得到密码口令。经常改密码。

5 SSID

以下是几条加强 SSID 安全的措施:

A 禁止发送

B 使唯一

C 经常改

绝大多数的网络设备都给你发送 SSID 选择，为了你下次登陆方便，很容易让任何人进入你的无线网络。这里也包括黑客。所以不要发布 SSID。
.
一个默认 SSID 在你的网络设备出厂就有了（LINKSYS 设备 SSID 是 LINKSYS）黑客知道了默认设置就能攻击你的网络。改变你的 SSID，使唯一，不要与产品厂家有联系。

经常改变 SSID 使黑客很难进入你的无线网络。

脑子里有这三个步骤，SSID 为了方便登陆网络，同时也容易受到网络黑客的攻击。

6 MAC 地址

如果你的无线产品可以，开启 MAC 地址过滤器。MAC 过滤器允许你进入无线节点用特定 MAC 地址。这让黑客很难用假的 MAC 地址或不常用的 MAC 地址进入网络。

7 防火墙

当你上互联网，你能用防火墙保护你的有线网络或无线网络。防火墙保护你的网络防止黑客进入。

8 WEP

WEP 是一种无线安全措施。这是 WEP 特有的功能。他让黑客变的更困难。

WEP 加密不仅有 802.11 标准，还有很多无线产品供应商提供的加密方法。另外，WEP 不是完善的安全措施。一条没加密的信息就是 MAC 地址，黑客可以用它来假冒 MAC 地址进入无线网络。

网上有很多程序可以击垮 WEP，最有名的是 AIRSNORT 程序，一天里，这个程序分析足够的传输数据，就好象统计分析攻击，最好的预防措施是不用固定设置，经常改变 WEP 密码，SSID 等。

以下几条可以让 WEP 功能最大化:

A 加密最高级

B 使用多重密码

C 按时改变 WEP 密码。

现在的加密技术是 64 位和 128 位加密技术，如果你是用 64 位加密，马上升级到 128 位。越复杂，越长，越好。WEP 密码两种方式: 1 一般的 WEP 密码　2 加密，解密都要通过网络。因此，具有较高的安全级别，黑客很难进入网络。

一个固定的 WEP 密码还是容易受到黑客攻击。你可以用多重 WEP 密码，加强无线网络安全。

我们知道 WEP 密码是存在无线卡片固件里，万一接入点被黑客侵入，则他们就得到了 WEP 密码，他们就可以侵入你的网络，用一个固定的 WEP 密码没有任何的保护意义。

解决的方法就是网络分层，如果你的网络有 80 个用户，你用 4 个 WEP 密码，你的黑客只有侵入你无线网络资源四分之一的可能。这样多个密码增加你的网络的可靠性。

最后，要经常改变 WEP 密码，一星期或一天一次，要使用动态 WEP 密码，使黑客很难进入你的无线网络资源

2.4GHZ/802.11G WEP 加密

为无线 G VPN 宽带路由器 WEP 加密是通过无线网络运用标签完成的，从标签上激活 WEP，点编辑 WEP 设置键，打开 WEP 窗口，如 B-3



图 B-2：WEP

从这个窗口，你可以选择 WEP 加密类型，再设置 WEP 密码。

当发送数据，则选 WEP1-4 密码中的一个，选择它为默认传输密码。确认接收设备也用同样密码。

选择 WEP 加密级别，64 位或 128 位，级别越高，越安全，加密复杂也会减缓网速。

如果你想用 WEP 护照，则最多输入 16 个字母数字字符。如果有非 LINKSYS 公司的产品这个护照可能就没用，因为和其他的设备在这一项上不兼容。可以手动输入 WEP 密码，或直接用护照字符。

如果你愿意手动输入 WEP 密码，确定在左边字段里密码类型。WEP 密码必须包含字母“A”到“F”和数字“0”到“9”，64 位 10 个字符，128 位 25 个字符长度。所有的网络节点必须在无线网络上使用同一 WEP 密码，使用 WEP 加密功能。

一旦输入护照字符，点 GENERATE 键去作为一个 WEP 密码输入进去。

当在标签上完成这些更改，点保存设置键去保存更改或点取消更改键使你的更改无效。

附录 C：配置 Windows 2000 计算机和路由器之间的互联网协议安全

引言

本资料介绍了如何使用预先共享的密码加入 VPN 路由器和 Windows 2000 或 XP 计算机内部的私人网络来确立一个安全的互联网协议安全隧道。

微软 KB Q25735-如何在 Windows 2000 内配制互联网协议安全隧道。
http://support.microsoft.com/support/kb/articles/Q252/7/35.asp

微钦 KB Q257225-Windows 2000 内基本的互联网协议安全的故障检修。
http://support.microsoft.com/support/kb/articles/Q257/2/25.asp



注意：请对所有的更改进行记录。
这些更改在 Windows“安全协议”应用和路由器的万维网的实用程序中是一样的。

环境

本附录中提及的 IP 地址和其它说明仅作解说之用。

Windows 2000 或 Windows XP
IP 地址：140.111.1.2<=用户互联网服务提供者提供 IP 地址；仅仅是一个例子。

分支网络掩码：255.255.255.0

BEFSX41

广域网 IP 地址：140.111.1.1<=用户互联网服务提供者提供 IP 地址；这仅仅是一个例子。

分支网络掩码：255.255.255.0
局域网 IP 地址：192.168.1.1
分支网络掩码：255.255.255.0

如何确立一个安全的互联网协议安全隧道

步骤 1：建立一个互联网协议安全策略

1. 单击“Start”（开始）钮，选择“Run”（运行），并在“Open”（打开）的字段输入“secpol.msc”，局部安全设置屏幕将会出现如图 C-1 所示。

2. 右键单击“IP Security Policies on Local Computer”（局部计算机上的 IP 安全策略）并单击“Create IP Security Policy”（建立 IP 安全策略）。

3. 单击“Next”（下一步）按钮，然后为你的策略输入一个名称（例如：to_router）然后单击“Next”（下一步）钮。

4. 撤消选定激活默认反应规则选择框，然后单击“Next”（下一步）按钮。

5. 单击“Finish”（完成）按钮，并确定已检验了“Edit”（编辑）选择框。

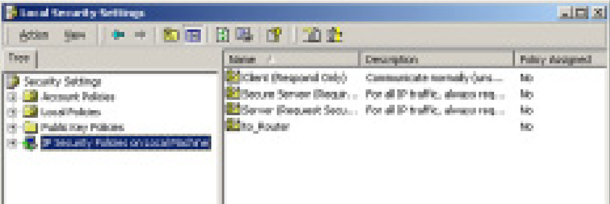


图 C-1：密码屏幕



注：本部分中涉及“窗口”内容以 Windows 2000 和 XP 为参照。

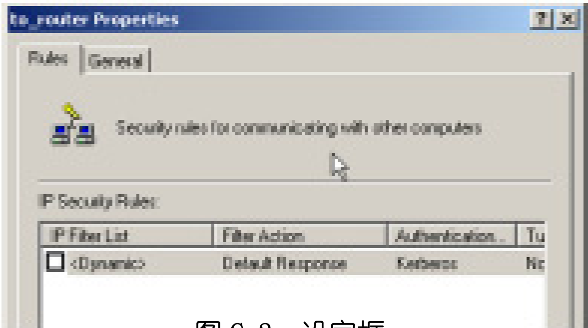


图 C-2：设定框

步骤 2：建立筛选表

筛选表 1：窗口->路由器

1. 在新策略的特征屏幕中，确认已选择了规则框，如图 C-2 所示。撤消选定“Use Add Wizard”（使用增加向导）选择框，并单击“Add”（增加）钮来建立一个新的规则。

2. 确认选择了 IP 筛选表，并单击“Add”（增加）钮。（见图 C-3）

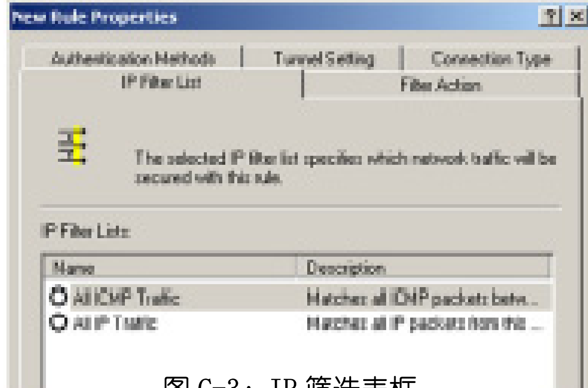


图 C-3：IP 筛选表框

3. 出现的 IP 筛选表屏幕必须如图 C-4 所示。为筛选表输入如“窗口->路由器”，之类的恰当名称，并撤消选定“Use Add Wizard”（使用增加向导）选择框。然后单击“Add”（增加）钮。

4. 出现的筛选特征屏幕必须如图 C-5 所示。选择地址框。在源地址字段选择“My IP”（我的 IP 地址）。在目的地址字段选择一个具体的 IP 分支网络，输入 IP 地址，192.168.1.0 和分支网络掩码 255.255.255.0。（这些是路由器的默认设置。如果你改变了这些设置，则必须输入新的数值）。

5. 如果想为你的筛选程序输入一个说明，单击“Description”（说明）框，并输入说明即可。

6. 单击“OK”钮，然后单击 IP 筛选窗口上的“OK”（用于 Windows XP）或“关闭”（用于 Windows 2000）钮。

筛选表 2： 路由器->窗口

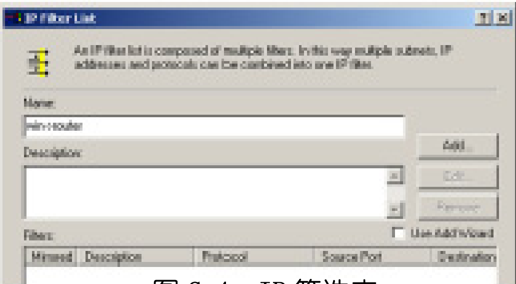


图 C-4：IP 筛选表

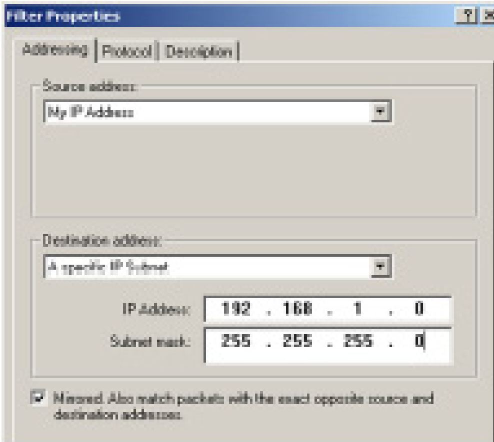


图 C-5：筛选特征

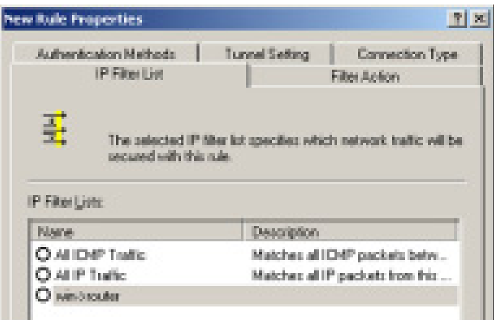


图 C-6：新规则特征

8. 出现的 IP 筛选必须如图 C-7 所示。为筛选表输入如“窗口->路由器”之类的恰当名称，并撤消选定“Use Add Wizard”（使用增加向导）选择框，然后单击“Add”（增加）钮。

9. 出现的筛选特征屏幕必须如 C-8 所示，选择地址框。在源地址字段选择一个具体的 IP 分支网络，并输入 IP 地址 192.168.1.0 和分支网络掩码 255.255.255.0（如果改变了默认设置则必须输入新的数值）。在目的地址中选择我的 IP 地址。

10. 如果想为你的筛选程序输入一个说明，单击“Description”（说明）钮并输入说明即可。

11. 单击“OK”键。出现的新规则特征屏幕必须带有已选的 IP 筛选表，如图 C-9 所示。此时，必须有一个有关“路由器->窗口”和“窗口->路由器”的列表。单击 IP 筛选表窗口上的“OK”（适用于 WinXP）或“Close”（适用于 Win2000）钮。

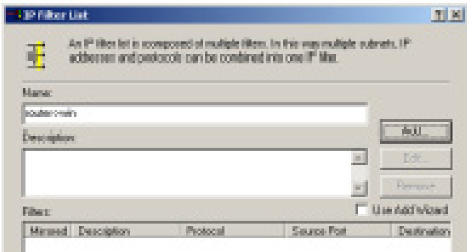


图 C-7：IP 筛选表

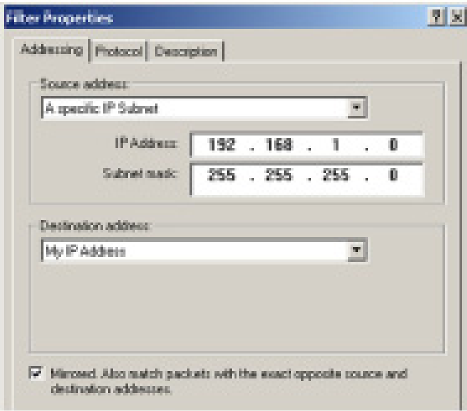


图 C-8：筛选特征

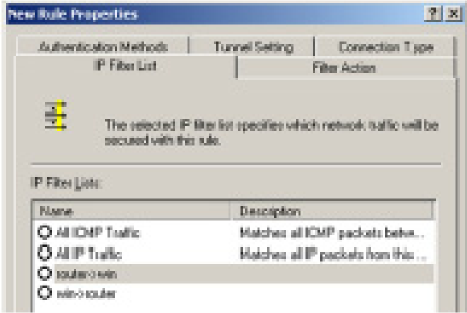


图 C-9：新规则特征

步骤 3：配置单个隧道规则

隧道 1：窗口->路由器

1. 如图 C-10 所示，从 IP 筛选表制表框上点击筛选表窗口->路由器。

2. 单击筛选行动框（如图 C-11 所示），并单击“Filter action Require Security radio”（筛选行动要求安全无线电）钮。然后单击“Edit”（编辑）按钮。

3. 如图 C-12 所示，从安全方法制表框中确认“协商安全选择”已启动，并撤消选择“Accept unsecured communication”（接受不安全的交流），但总是利用互联网协议安全选择框作出反应。选择“Session Key Perfect Forward Secrecy”（对话密码完美正向保密）并单击“OK”钮。

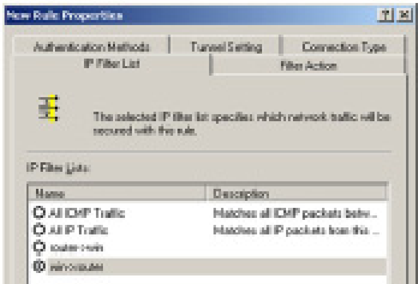


图 C-10：IP 筛选表框

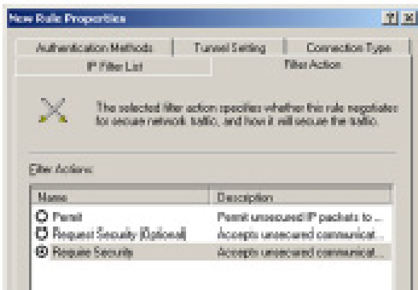


图 C-11：筛选行动框

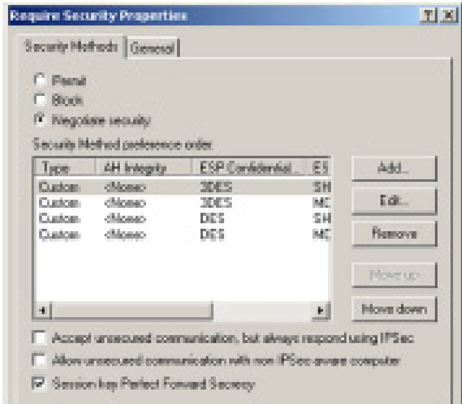


图 C-12：安全方法框

4. 选择“Authentication Methods”（鉴别方法）制表框，如图 C-13 所示，并点击“Edit”（编辑）钮。

5. 将鉴别方法改成“使用本字符串保护密码交换（预先共享的密码)”如图 C-14 所示，并输入预先共享的密码字符串，如 XYZ12345。单击“OK”钮。

6. 图 C-15 中将展示该预先共享的新密码。点击“OK”或“Close”（关闭）钮。

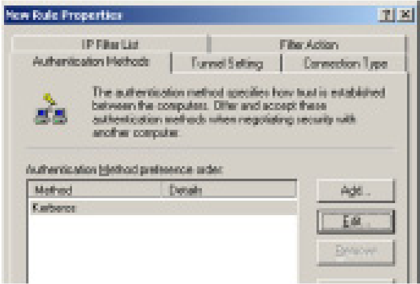


图 C-13：鉴别方法

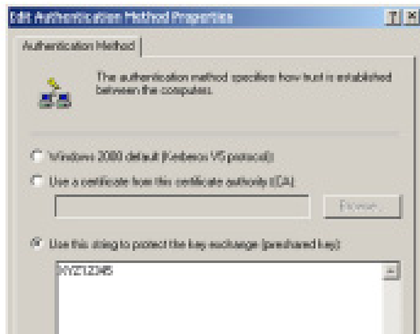


图 C-14：预先共享的密码

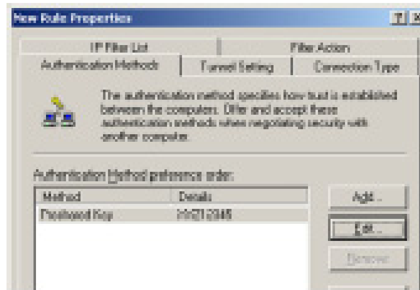


图 C-15：预先共享的新密码

7. 选择“Tunnel Setting”（隧道设置）框，如图 C-16 所示。单击“The tunnel endpoint is specified by this IP Address”（隧道端点由本 IP 地址指定）无线电按钮，然后输入路由器的广域网 IP 地址。

8. 选择“Connection Type”（连接类型）框，如图 C-17 所示。单击“All network connections”（所有网络连接），然后单击“OK”或“Close”钮，结束本规则。

隧道 2：路由器->窗口

9. 在新策略的特征屏幕上，如图 C-18 所示，确认选择“win->router”（窗口->路由器）并撤消选择“Use Add Wizard”（使用增加向导）选择框。然后单击“Add”（增加）钮建立第二个 IP 筛选程序。

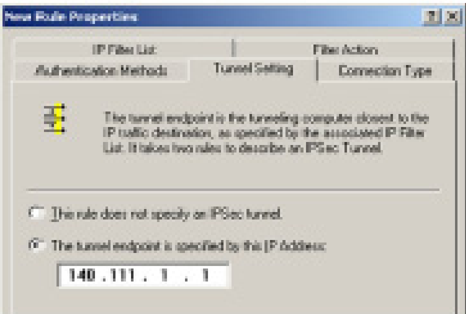


图 C-16：隧道设置框

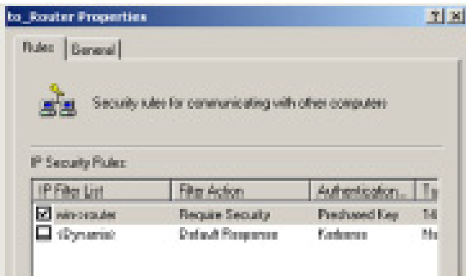


图 C-17：连接类型框

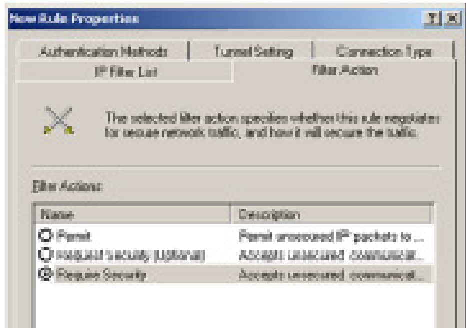


图 C-18：循征屏幕

10. 进入“IP Filter List”（IP 筛选表）框，单击“the filter list router->win”（筛选表路由器->窗口），如图 C-19 所示。

11. 单击“Filter Action”（筛选行动）框，选择筛选行动“Require Security”（要求安全），如图 C-20 所示，然后单击“Edit”（编辑）钮。

12. 单击“Authentication Methods”（鉴别方法）框，并确认选择 Kerberos 鉴别方法，如图 C-21 所示，然后点击“Edit”（编辑）钮。

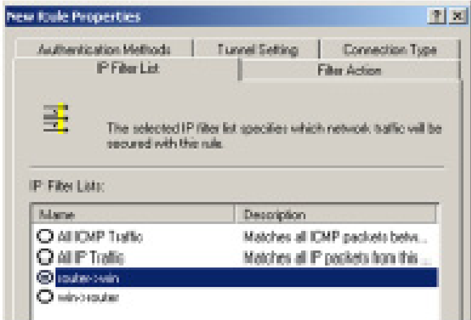


图 C-19：IP 筛选表框

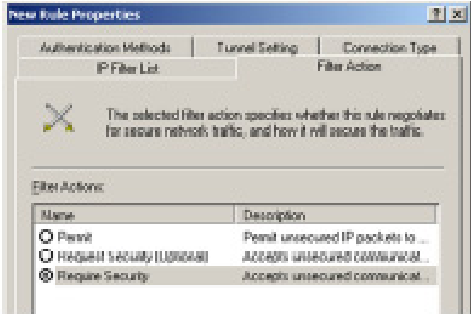


图 C-20：筛选行动框

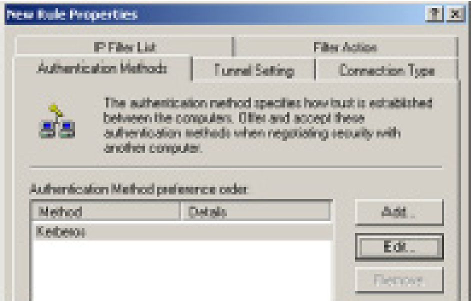


图 C-21：鉴别方法框

13. 将鉴别方法改成“Use this string to protect the key exchange (preshared key)”（使用本字符串保护密码交换（预先共享密码）），并输入预先共享的密码字符，例如：XYZ12345，如图 C-22 所示。（这只是一人密码字符样本。你的密码字符必须独特又容易记）。然后单击“OK”钮。

14. 图 C-23 中将显示新的预先共享的密码。单击“OK”钮继续。

15. 从图 C-24 所示的隧道设置框中，单击无线电钮以确定隧道的端点由本 IP 地址指定，然后输入 Windows 2000/XP 计算机的 IP 地址。

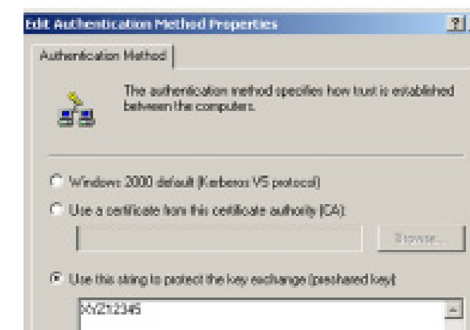


图 C-22：预先共享的密码

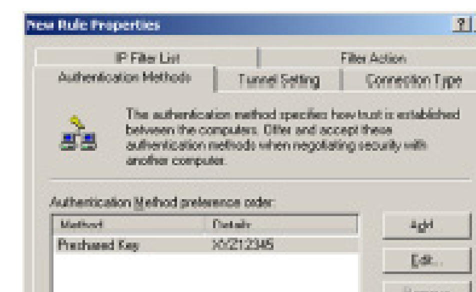


图 C-23：预先共享的新密码

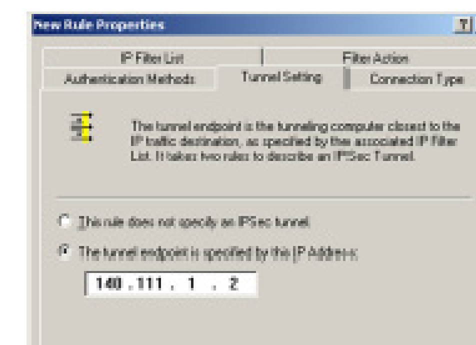


图 C-24：隧道设定框

16. 单击“Connection Type”（连接类型）框，如图 C-25 所示，选择“All network connections”（所有网络连接），然后单击“OK”（适用于 Windows XP）或“Close”（适用于 Windows 2000）钮结束。

17. 在图 C-26 所汇款单的规则框中，单击“OK”钮以返回第二个屏幕。

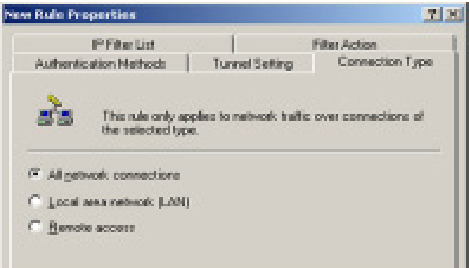


图 C-25：连接类型

步骤 4：指定新的互联网协议安全策略

在局部计算器窗口上的 IP 安全策略中，如图 C-27 所示，右键单击名为“to_router”（到_路由器）的策略，并单击“Assign”（指定）。一个绿色箭头则出现在文件夹图标中。

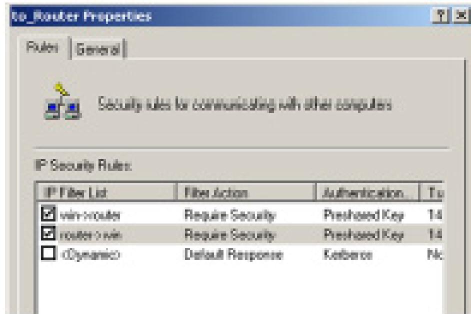


图 C-26：规则

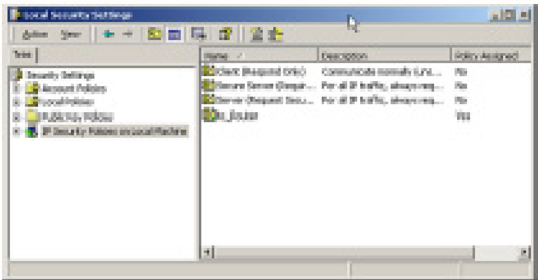


图 C-27：局部计算机

步骤 5：通过以万维网为基础的实用程序建立一个隧道

1. 打开万维网浏览器，在地址字段输入 192.168.1.1 按“Enter”（回车）键。

2. 当用户名称和密码字段出现时，输入默认用户名和密码“admin”，按“Enter”（回车）键。

3. 在“Setup”（设置）框中，单击 VPN 框。

4. 从如图 C-28 所示的 VPN 框中，选择你希望在“选择隧道入口下拉框”建立的隧道，然后单击“Enabled”（启动），在隧道名称字段输入隧道名称。这使得你可以识别多种隧道，而且不须匹配隧道另一端使用的名称。

5. 在局部安全组字段输入局部 VPN 中币器的 IP 地址和分支网络掩码。为了能够进入 IP 分支网络，IP 地址最后的数字输入为 0（例如：192.168.1.0）。

6. 在远程安全网关字段中隧道的另一端（远程 VPN 路由器或你希望用之交流的装置）输入 VPN 装置的 IP 地址和分支网络的掩码。

7. 从两种不同类型的加密 DES 或 3DES 中选择（推荐采用 3DES，因为它更安全），你可以选择其中任何一个，但其必须和隧道另一端 VPN 装配使用的加密类型一样。或者你也可以选择“禁用”不进行加密。

8. 从两种难方式 MD5 或 SHA 中选择（建议采用 SHA，因为它更安全）。和加密一样，如果另一端隧道的 VPN 装置使用了相同的鉴定方法，你可以选择其中任何一个。或者隧道两端均可选择禁用验证。

9. 选择数码管理，选择“自动”（IKE），并在预先共享密码字段输入一连串的数字或字母。检查靠着 PFS（完美正向保密）的字框以确定初始的密码交换和 IKE 建议是安全的。在本字段，你可以采用 24 个数字或字母的任何组合，不允许特殊字符或空隔。在密码寿命字段，你可以任意让密码在你选择的时间段末尾到期。输入你希望密码有用的秒数或保持空白，让密码无限期有效。

10. 单击“Save Settings”（保存设置）钮，保存这些改变。

现在，你的隧道就已经确立了。



图 C-28：VPN 框

附录 D：找出以太网适配器的 MAC（介质访问控制）地址和 IP 地址

本部分讲述了如何找到计算机以太网适配器的 MAC 地址，这样你就可以使用路由器的 MAC 筛选和/或 MAC 地址兼容的特征。你也可以找到计算机以太网适配器的 IP 地址。该 IP 地址用于路由器的筛选、发送和/或 DMZ 特征。按本附录的步骤找出 Windows 98, Me, 2000 或 XP 适配器的 MAC 或 IP 地址。

Windows 98 或 Me 指令

1. 单击“Start”（启动）和“Run”（运行）钮，在空白区域输入“winipcfg.”，然后按回车键或单击“OK”钮。

2. 当 IP 配置屏幕出现时，选择你已通过 CAT 与以太网网络电缆连接到路由器上的以太网适配器。见图 E-1。

3. 写下计算机屏幕所示的适配器地址（见图 E-2），这就是以太网适配器的 MAC 地址，它以一连串数字和字母方式出现。

MAC 地址/适配器地址就是你将用作 MAC 地址兼容或 MAC 筛选的地址。

图 E-3 中所示例子显示以太网适配器的 IP 地址为 192.168.1.100。你的计算机显示的可能会有的不同。



注：MAC 地址也称适配器地址。

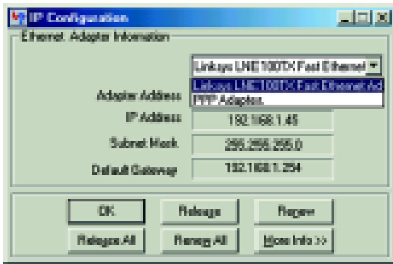


图 D-1：IP 配置屏幕

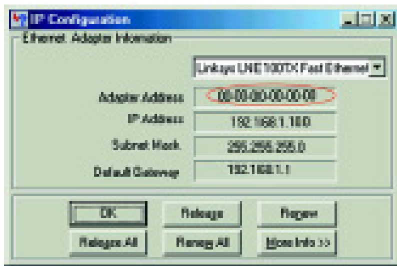


图 D-2：MAC 地址/适配器地址

Windows 2000 或 XP 指令

1. 单击“Start”（启动）和“Run”（运行）钮。在空白区域输入 cmd。按“Enter”（回车）键或单击“OK”钮。



注：MAC 地址也称实际地址。

2. 在命令提示栏中输入 ipconfig/all。然后按“Enter”（回车）键。

3. 写下计算机屏幕所示的实际地址（图 E-3）；这是你的以太网适配器的 MAC 地址。它以一连串的数字和字母形式出现。

MAC 地址/实际地址是你将用来 MAC 地址兼容或 MAC 筛选的地址。

图 E-3 中的例子显示的以太网适配器的 IP 地址为 192.168.1.100。你的计算机显示的可能会有所有同。

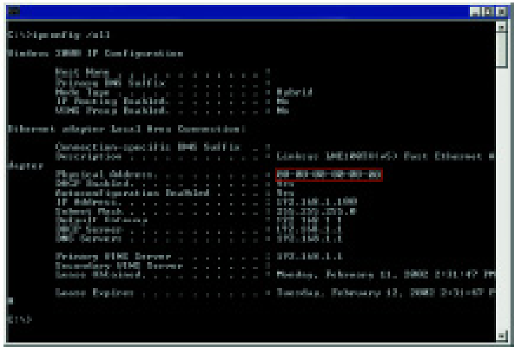


图 D-3：MAC 地址/实际地址

附录 E：SNMP（简单网络管理协议）功能

SNMP（简单网络管理协议）是一种广泛使用的网络监控协议。数据从一个 SNMP 主体，例如 VPN 路由器传到用于监视网络的工作站控制台，路由器然后包含在 MIB（管理信息库）里的信息。该 MIB 是一个定义什么可以从装置中获取以及什么可以控制的（关、开等）数据结构。

如果没有第三方的管理软件，就不能提供如统计、配置以及装置信息之类的 SNMP 功能，路由器与所有 IP 开放视图顺应性软件兼容。

附录 F：升级固件

路由器的固件升级是通过管理框上万维网实用程序的固件升级框来完成的。

1. 单击浏览钮，找出你从链接系统的网站上下载并抽取的固件升级文档。

2. 双击所下载并抽取的固件文档，单击升级钮，然后按指令进行。



图 F-1：升级固件

附录 G：Windows 帮助

所有的无线产品均要求微软 Windows，windows 是世界上使用最为广泛的操作系统，它的很多特征有助于使网络更多简单。可以通过 Windows 帮助进入这些特征，具体如本附录所述。

TCP/IP（传输控制协议/互联网协议）

在计算机和接入点交流之前，必须启动 TCP/IP。TCP/IP 是一组指令或协议，所有个人计算机均按照它们进行网络交流。对无线网络也一样，不启动 TCP/IP，你的计算机就不能使用无线网络，Windows 帮助提供了启动 TCP/IP 的全部指令。

共享资源

如果你想通过网络共享打印机、文件夹或文档，Windows 帮助提供了有关利用共享资源的所有指令。

网络邻居/我的网络地点

你网络中的其它计算机会出现在“网络邻居”或“我的网络地点”目录下（取决于你运行的 Windows 版本）。Windows 帮助提供了有关如何将计算机加入你的网络的所有指令。

附录 H：词汇表

802.11a – 一种规定了最大的数据传送率为 54Mbps，操作频率为 5GHz 的 IEEE（电气和电子工程师学会）无线网络标准。

802.11b – 一种规定了最大数据传送率为 11bps，操作频率为 2.4GHz 的 IEEE 无线网络标准。

802.11g – 一种规定了最大数据传送率为 54Mbps，操作频率为 2.4GHz 以及与 802.11b 装置反向兼容性的 IEEE 无线网络标准。

接入点 – 允许无线计算机和其它装置与有线网络交流的装置，也可以用来扩展无线网络的范围。

适配器 – 该装置将网络功能性增加到你的计算机中。

Ad-hoc – 不使用接入点就可以直接相互交流的一组无线装置。

中枢 – 连接大多数系统和网络并处理大多数数据的部分网络。

带宽 – 给定装置或网络的传输能力。

信标区间 – 信标的频率区间，是一种通过路由器广播来同步无线网络的信息包。

位 – 二进制位。

引导 – 启动装置并使之，开始执行指令。

桥接器 – 连接两种不同局域网络的装置，例如连接无线网络和有线以太网网络。

宽带 – 始终连接快速的连接法。

浏览器 – 浏览器是一种提供在万维网上查看并与所有信息相互影响的一种应用程序。

缓冲器 – 当装置当前太忙而不能接受数据时临时保存后期处理数据的一种记忆块。

电缆调制解调器 – 将计算机与电缆电视网络连接该网络依次连接互联网的一种装置。

CSMA/CA（载波监听多址访问/冲突避免）– 用来防止互联网数据遗失的一种数据传输方法。

CTS（清除发送） – 一种由装置发送表示准备接收数据的信号。

菊花链 – 一种用来按顺序连接装置的方法，一个接一个。

数据库 – 可以很容易进入、管理并更新的一种数据集。

DDNS（动态域名系统） – 拥有一个网站，FTP（文件传送协议）或带有动态 IP 地址-使用一个固定域名的电子邮件服务器的容量。

默认网关 – 从局址网传送互联网通信量的一种装置。

DHCP（动态主机配置协议）– 允许局域网上存在一个装置，即 DHCP 服务器，将临时 IP 地址分配到其它网络装置，特别是计算机上的一种协议。

DMZ（非军事化区域）– 清除一台计算机上的路由器防火墙保护，允许从互联网上可以“看见”该计算机。

DNS（域名服务器）– 互联网服务器提供者服务器的 IP 地址，该服务器将网站的名称翻译成 IP 地址。

域 – 计算机网络的具体名称。

下载 – 接收通过网络传输的文档。

DSL（数字用户线路）– 通过传统电话线随时连接的宽带连接法。

DSSS（直接顺序扩展频谱）– 一种无线电传输技术，它含有一个多余位模式来减少传输期间数据丢失的可能性。用于 802.11b 网络。

DTIM（传递通信指示信息）– 包含在数据包中并可以提高无线效率的信息。

动态 IP 地址 – DHCP 服务器指定的一个临时 IP 地址。

加密 – 编码数据防止未授权人阅读。

以太网 – 指定数据如何放置并如何从传输媒介检索的一个 IEEE 标准网络协议。

Finger 命令 – 告诉你与一个电子邮件地址相关名称的一种程序。

防火墙 – 保护局域网域资源不受外界侵入的安全措施。

固体 – 1. 在网络装置中运行装置的程序。2. 装载在只读内存（ROM）或不能被终端用户改动的可编程只读内存（PROM）上的程序。

分段 – 在通过不能支持信息包原本尺寸的网络媒体进行传输时，将信息包分成各个小单元。

FTP（文件传递协议）– 通过 TCP/IP 和互联网在计算机之间发送文档的一种标准协议。

全双工 – 联网装置同时接收和传输数据的能力。

网关 – 互相连接网络的一种系统。

半双工 – 通过单线可以出现在 2 个方向，但一个时间段仅出现在一个方向的数据传输。

硬件 – 计算机远程通信技术及其它信息技术装置的实物方面。

HTTP（超文本传送协议）– 用来连接万维网上服务器的通信协议。

IEEE（电气和电子工程师协会）– 开发联网标准的独立协会。

信息基础结构设施 – 当前安装的计算和联网的设备。

信息基础结构设施模式 – 通过接口点将无线网络与有线网络进行桥接的配置。

IP（互联网协议）– 通过网络发送的一种协议。

IP 地址 – 用来识别网络上计算机或装置的地址。

IP 配置 – 向特殊联网装置展示 IP 地址的一种 Windows 2000 和 XP 实用程序。

IPSec（互联网协议安全）– 用来执行 IP 层次上信息包安全交换的一种 VPN 协议。

ISM 波段 – 用于无线互联传送的无线波段。

ISP（互联网服务提供者）– 提供进入互联网的公司。

局域网（LAN）– 在你的家中或办公室里形成网络的计算机和联网产品。

MAC（介质访问控制）地址- 制造商分配给各联网装置的独特地址。

Mbps（兆位每秒）– 每秒 100 万进位；测量数据传送的单位。

多数据类型转换 – 立即将数据传送到一组目的地。

NAT（网络地址翻译）– NAT 技术将一个局域网的 IP 地址为互联网翻译成一个不同的 IP 地址。

网络 – 一系列计算机或装置连接起来，在用户之间共享存储和/或传输数据。

NNTP（网络新闻传递协议）– 用来连接互联网上用户网的协议。

网点 – 一个网络节或连接点，典型地如一台计算机或工作站。

OFDM（正交频率除法多路转换技术）– 将数据流分成许多低速数据流并进行平行传输的一种调制技术。用于 802.11a、802.11g 和电源线联网。

信息包 – 通过网络发送的一种数据单元。

□令短语 – 作用非常像密码，□令短语通过自动生成铰接系统产品 WEP 加密密码来简化 WEP 加密过程。

Ping（互联网信息包搜寻协议）– 用来确定某个特定 IP 地址是否在线的互联网应用程序。

POP3（邮电局协议 3）– 用来检索存储在邮件服务器上的一种标准协议。

端□ – 1. 用于插入电缆或适配器上的计算机或互联装置上的连接点。2. 虚拟连接点，计算机通过该点在服务器上的一个具体应用。

PPPoE（以太网的点到点协议）– 数据传输之外还提供识别（用户名和密码）功能的一种宽带连接。

PPTP（点到点隧道协议）– 允许噗到点协议（PPP）通过 IP 网络传送的一种 VPN 协议。该协议在欧洲也用作一种宽带连接。

前同步码 – 同步网络通信的部分无线信号。

RJ-45（注册插口-45）– 可以连接 8 根线的以太网适配器。

移像 – 将无线装置从一个接入点的区域带到另一个区域而不会失去连接的能力。

路由器 – 连接多个网络的联网装置，例如连接局域网和互联网。

RTS（请求发送）– 计算机有信息要输送时发出的信息包。发送数据之前计算机将等待一个 CTS（清除发送）命令。

服务器 – 在网络中能够让用户访问文档、打印、通信和其它服务的任一计算机。

SMTP（简单电子邮件传递协议）– 互联网上的标准电子邮件协议。

SNMP（简单网络管理协议）– 一种广泛使用的网络监控协议。

软件 – 计算机所用的指令。执行某个特定任务的一系列指令称为“程序”。

扩展频谱 – 用于更可靠更安全数据传输的宽带无线频率技术。

SSID（服务设置标识符）– 你的无线网络名称。

固定 IP 地址 – 指定给与网络连接的计算机或装置的一种固定地址。

固定发送 – 通过固定的路径在网络中传送数据。

分支网络掩码 – 决定网络大小的地址码。

开关 – 1. 网络中连接计算机和其它装置的中心点，这样数据可以以全速传输进行共享。2. 电路中连接、切断或改变连接的一种装置。

TCP/IP（传输控制协议/互联网协议）– 传输的数据必须得到数据接收者确认的一种网络协议。

远程登陆 – 用于处理远程计算机的一种用户命令和 TCP/IP 协议。

TFTP（普通文档传送协议）– 使用 VDP 且没有目录或密码容量的 TCP/IP FTP 协议的一个版本。

吞吐量 – 在特定时间段内，从一个网点成功传到另一个网点的数据量。

布局技术 – 网络的实际布局。

TX 率 – 传输率。

UDP（用户数据协议）– 传输的数据不需要数据接收者确认的一种网络协议。

升级 – 用更新的版本替换已有的软件或固件。

URL（统一联网地址）– 文件在互联网上的地址。

VPN（虚拟私人网络）– 数据在互联网上离开一个网络进入另一个网络时保护该数据的一种安全措施。

WAN（万维网）– 互联网。

WEP（有线等效保密）– 在无线网络传输时，为了更加安全而对传输数据进行加密的一种方法。

WINIPCFG – 向某种专门联网设置显示 IP 地址的一种 Windows 98 和千年应用程序。

WLAN（无线局域网）– 一组相互无线通信的计算机和相关装置。

附录 I：技术说明

标准	IEEE802.3，802.11b 和 802.11g
端口	一个互联网，以太网（1-4），电源
按键	一个重设键，一个电源开关
电缆型号	UTP CAT5 或更好的
数据速率	达到 54Mbps
输送电源	19dBm
LEDs（指示灯）	电源、互联网、以太网（1,2,3,4），无线-G，DMZ
安全特征	WEP，802.1 x 监别
WEP 健位	64,128
尺寸 （W x H x D）	7.32” x 6.89” x 1.89” (186mm x 175mm x 48mm)
装置重量	1.26 lb（0.57kg）
电源	外置，5V 交流电，2.5A
认证	FCC，IC-03
操作温度	0^{0}C 到 40^{0}C（32^{0}F 到 104^{0}F）
储存湿度	-20^{0}C 到 70^{0}C（-4^{0}F 到 158^{0}F）
操作温度 存储湿度	10%到 85% 无凝结 5%到 90% 无凝结

附录 J：保修信息

有期限的保修

Linksys 向原始终端用户购买者（“您”）保证：在 3 年时间里（“保修期”），Linksys 产品在正常使用情况下不会产生材料或工艺的缺陷，在本保修期内，如果您的产品发生问题且完全是 Linksys 的责任，我们将毫无争议地选择修理、替换本产品或补偿您的购买价格。

如果保修期间产品发生问题，请拨打 Linksys 的技术支持电话以获取一个退还确认号。拨打电话时一定要把购买凭证带在身边。退回产品时，将退还确认事情清晰地标上包裹上并附上原始购买凭证的复印件。没有购买凭证则不能处理退还要求。您有义务将故障产品运到 Linksys 公司，Linksys 只负责通过 USP 将产品返还给您的地面费用。美国和加拿大以外的客户负责所有的发运和操作费用。

所有有关可购买性或适用特定目的的，暗示保修条件只限于保修期间。不承认所有其它明确的或暗示的条件、陈述及保修情况，包括任何暗示性的非侵犯保修情况，有些司法规定不允许对暗示性的保修存在时间进行限制，所以上述的限制可能不适用于您。本保修书给了您详细的合法权利，根据司法的不同您可能还享受其它的权力。

在法律没有禁止的范围上，Linksys 决不承担由于特殊间接的、推论性的、偶然的或惩罚性的损坏而产生的数据丢失，收入或利益损失的责任。不管这些损失是否由可靠性原理、使用本产品或与本产品有关的东西或不能使用本产品，而造成的，哪怕是 Linksys 已接到关于这些损坏可能性的通知，Linksys 的责任决不会超过您购买本产品所支付的费用。

前面的限制也适用于本章节所提及的任何保修或补偿不能实现其基本目的的情况。有些司法不允许排除或限制偶然性或推论性的损坏，所以上述的排除情况或限制可能不适用您。

如果有问题，请直接联系我们。

附录 K：规章信息

FCC（联邦通信委员会）声明

根据 FCC 制度第 15 部分，本产品已经过测试并符合 B 级数字装置的技术要求。这些限制是为了提供合理的保护以防止固定安装时产生有害的干扰。本设备产生利用并能发生无线频率能量。如果没有根据说明进行安装和作用，可能会对无线通信产生有害的干扰。但是，我们并不保证特定安装情况下不公出现干扰。如果开关本设备时发现本设备真的对无线或电视接收产生了有害干扰，我们鼓励用户采用下列一个或多个措施改正干扰。

- 改变接收天线的方向或重新定位接收天线。
- 提高设备之间或装置之间的间隔。
- 将设备连接到出口上，而不是接收器上。
- 向中间商或有经验的无线/电视技工。

FCC 辐射暴露声明
本设备符合针对不受控制的环境，设定的 FCC 辐射暴露限制。设备的安装和操作必须在辐射器和人体之间至少间隔 20cm 的情况下进行。

待业加拿大（加拿大）
本 B 级数字装置符合加拿大 ICES-003。
如果本装置用于部分或全部室外操作的系统中，则可能要求用户根据加拿大规章取得该系统的许可证。

EC 合格声明（欧洲）
Linksys 集团声明包含在快速无线™系列中的快速无线™系列产品符合下列所列的技术说明，符合 EMC 指令 89/336/EEC 和低压指令 73/23/EEC 的条款。

无线设备的 EMC 通用要求 ETS300-826,301 489-1

安全 EN609 50
无线设备的技术要求 ETS300-328-2

注：本设备可用于所有欧盟和 EFTA 国家。室外使用可能限制到某些频率和/或可能会要求操作许可证。更多详细细节请联系 Linksys 公司相应部门。

注：电源级别和天线的结合导致放射电源级别达到 100mW 以上，这种情况被视为不符合上述的指令，不得用于欧盟国家及那些采用欧洲 R&TTE 指令 1999/5/EC 和/或 CEPT 建议 Rec70.03 的国家。有关电源级别和天线的合法结合情况，请联系 Linksys 公司相关部门。

法国 F：频率波段，只有频道 10,11,12,13（名为 2457,2462,2467 和 2472 赫兹）可以用于法国。所有室内和室外安装均要求许可证。有关要遵守的程序，请联系 ART。

德车 D：室外安装要求许可证。有关要遵守的程序请查询转卖商。

意大利 I：室内安装要求许可证。不允许进行室外安装使用。

荷兰：要求室外安装的 NL 许可证。有关要遵守的程序，请查询转卖商。

附录 L：联系信息

需要联系 Linksys 吗？
有关最新产品的信息及更新您已有的产品请参观我们的网站：

www.linksys.com/cn

不能在网上找到您想购买的产品信息吗？
您相知道与 Linksys 产品联网的更多信息吗？
给我们的建议组打个电话至：

(8610) 6526 7777

如果您在使用 Linksys 产品时发现任何问题，请拨打我们的电话：

(8610) 6526 7777
chinasupport@linksys.com

如果在保修期间发现产品有任何故障，您可以联系 Linksys，
以获取一个返还认可号。联系电话为： (8610) 6526 7777
（有关保修和 RMA 问题的细节可以在本说明的保修信息部分查到）